UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH

Application for JPEG privacy implementation with XACML

A Degree Thesis

Submitted to the Faculty of the

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Miguel Castillo Nolasco

In partial fulfilment

of the requirements for the degree in

Audiovisual Systems Engineering

Advisor: Jaime M. Delgado Merce

Barcelona, February 2017

Abstract

This project is based on the development of an application for the management of privacy and security in JPEG images through policies designed in standard XACML

The privacy policies are incorporated into the metadata defined for this type of data in the JPSearch standard for the compaction of the information in a single resource.

Dynamic queries (request) are generated with the purpose of obtaining permission to access an image by checking the privacy policies, where it is determined who, how and when can access. The evaluation of the request against the policy is carried out by Balana, and this return an answer (response) with the decision.

There are three independent lines of work, firstly, the design and creation of privacy policies based on the XACML standard, secondly, the update of JPSearch metadata in the corresponding fields for privacy and security and, as a last part, the definition of the system for the validation of a request to an image through the Balana implementation that incorporates the architecture defined in XACML.

Resum

Aquest projecte mostra el desenvolupament d'una aplicació per a la gestió de la privacitat i seguretat en imatges JPEG a partir de polítiques dissenyades en l'estàndard XACML.

Les polítiques de privacitat estan incorporades a les metadades definides per aquest tipus de dades a l'estàndard JPSearch per a la compactació de la informació en un sol recurs.

S'han generat consultes dinàmiques (request) amb l'intenció d'obtenir el permís d'accés a una imatge comprovant les polítiques de privacitat, on es determina qui, com i quan pot accedir. L'avaluació de la request contra la política la realitza Balana, i aquest ens torna una resposta (response) amb la decisió.

Hi han tres línies de treball independents, en primer lloc, el disseny i creació de polítiques de privacitat a partir del estàndard XACML, en segon lloc, l'actualització de les metadades de JPSearch en els camps corresponents per a la privacitat i seguretat i com a última part la definició del sistema per a la validació d'una petició a una imatge a través de l' implementació Balana que incorpora l'arquitectura definida en l'estàndard XACML.

Resumen

Este proyecto muestra el desarrollo de una aplicación para la gestión de la privacidad y seguridad en imágenes JPEG a partir de políticas diseñadas en el estándar XACML.

Las políticas de privacidad son incorporadas en los metadatos definidos para este tipo de datos en el estándar JPSearch para la compactación de la información en un solo recurso.

Se generan consultas dinámicas (request) con la intención de conseguir el permiso de acceso a una imagen comprobando las políticas de privacidad, donde se determina quién, cómo y cuándo puede acceder. La evaluación de la request contra la política lo realiza Balana, y este nos devuelve una respuesta (response) con la decisión.

Hay tres líneas de trabajo independientes, en primer lugar, el diseño y creación de políticas de privacidad a partir del estándar XACML, en segundo lugar, la actualización de los metadatos de JPSearch en los campos correspondientes para la privacidad y seguridad y como última parte la definición del sistema para la validación de una petición a una imagen a través de la implementación Balana que incorpora la arquitectura definida en XACML.

Acknowledgements

I want to thank my director Jaime Delgado for giving me the opportunity to carry out this project. He has always provided me with the help and advice to overcome stages of difficulty during the project.

I also want to thank my family, friends and Laura for the mental support during these years of career.

Revision history and approval record

Revision	Date	Purpose
0	23/12/2017	Document creation
1	05/01/2018	Document revision
2	22/01/2018	Document revision

DOCUMENT DISTRIBUTION LIST

Name	e-mail
Miguel Castillo	mcastillonolasco@gmail.com
Jaime Delgado	jaime.delgado@ac.upc.edu

Written by:		Reviewed and approved by:	
Date	23/12/2017	Date	22/01/2018
Name	Miguel Castillo	Name	Jaime Delgado
Position	Project Author	Position	Project Supervisor

Table of contents

List of Figures

List of Tables

1. Introduction

1.1. Statement of purpose

Currently, a lot of different JPEG images are shared due to the ease of creating them, using a camera taking a picture or even creating a file on a computer. The images travel through networks with great ease due to current technology. Privacy and security in these cases is non-existent, which is why it motivates the management of these areas.

This project consists of the development of an application for the privacy of JPEG images through security policies based on XACML language. The objective is a functional system that implements these technologies and demonstrates how the cases of privacy in images can be solved.

The project main goals are:

- Functional system with privacy policies in images JPEG.
- Evaluate access requests according to the rules defined in policies.
- Use of the XACML language for the creation of policies and for sending the requests.
- Integrate the policies in the metadata of the JPEG images.
- Establish practical examples for the use of the system
- Provide the system with maximum security possible with encryption and digital signature

1.2. Requirements and specifications

Project requirements:

1. Authorize or deny access according to the policy of the image
2. Encryption of the privacy policy
3. Inclusion of the digital signature
4. Variety of privacy policies that can be tested
5. Environment of access to images for a registered user

Project specifications:

1. Database with the information of users and images
2. Local or cloud storage for images
3. Use of the XACML protocol
4. Application designed with IDE Eclipse
5. Inclusion of the policies in the metadata of the image with the program "JPEGMetadataEditor"
6. Use Balana open source implementation based on XACML standard.

1.3. Methods and procedures

Based on previous projects, the first one "Metadata Interoperability with JPSearch" of the student Nicos Demetriou to modify metadata of a image. Later this application was modified for its adaptation to privacy metadata in the project "Privacy in images jpg by XACML" of the student Alberto Durán Montoro. This project finally generates a policy and authorization in a simple case in a desktop application with a static request.
This project consists of going a step further and completing an access system through the standard (XACML). In short, a user can verify that the system really works for the privacy of the images
The XACML standard, the Balana implementation and the Eclipse IDE will be used to build the described application in Java.

1.4. Work plan

1.4.1. Tasks

<table>
<tr><td>Project: Application for JPEG privacy implementation with XACML</td><td colspan="2">WP ref: (WP#) 1</td></tr>
<tr><td>Major constituent: Search information</td><td colspan="2">Sheet 1 of 5</td></tr>
<tr><td rowspan="2">Short description:
Search information about the technologies.</td><td colspan="2">Planned start date: 01-09-17
Planned end date: 01-10-17</td></tr>
<tr><td colspan="2">Start event: 01-09-17
End event: 07-10-17</td></tr>
<tr><td>Internal task T1: Search information: XACML and Balana
Internal task T2: Search information: MySQL and Storage
Internal task T3: Search information: JavaEE and Web App
Internal task T4: Search information: Cryptography and Signature</td><td>Deliverables:

None</td><td>Dates:7

None</td></tr>
</table>

<table>
<tr><td>Project: Application for JPEG privacy implementation with XACML</td><td>WP ref: (WP#) 2</td></tr>
<tr><td>Major constituent: Desgin application</td><td>Sheet 2 of 5</td></tr>
<tr><td rowspan="2">Short description: Propose the design of application, estimate storage, databases, others…</td><td>Planned start date: 25-09-17
Planned end date:15-10-17</td></tr>
<tr><td>Start event: 25-09-17
End event: 15-10-17</td></tr>
</table>

Internal task T5: Use JPEGMetadataEditor Internal task T6: Design structure Web App Internal task T7: Create Database Internal task T8: Definition of storage for images	Deliverables: None	Dates: None

Project: Application for JPEG privacy implementation with XACML	WP ref: (WP#) 3	
Major constituent: Use of balana and privacy policies	Sheet 3 of 5	
Short description: Learn to use the Balana tool and design privacy policies	Planned start date: 15-10-17 Planned end date: 10-11-17	
	Start event: End event:	
Internal task T9: Create policies for request. Internal task T10: Do an a simple authorization	Deliverables: None	Dates: None

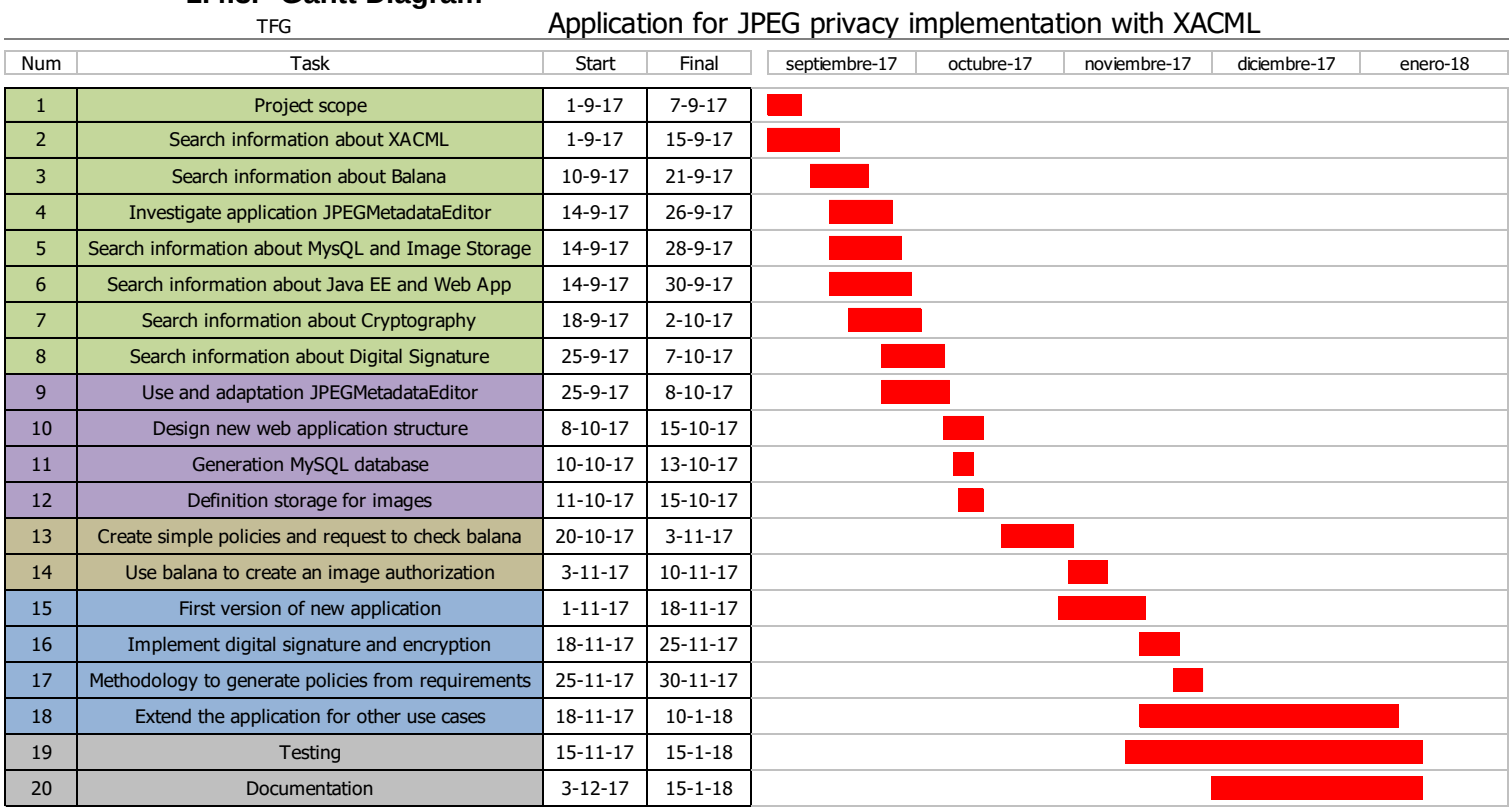
Project: Software prototype: Application for JPEG privacy implementation with XACML	WP ref: (WP#) 4	
Major constituent: Programming the main application	Sheet 4 of 5	
Short description: Program the web application and use of the system.	Planned start date: 08-10-17 Planned end date: 15-01-18	
	Start event: 08-10-17 End event: 10-01-18	
Internal task T11: First version web app Internal task T12: Digital signature and encryption Internal task T13: Methodology for create policies from requierements Internal task T14: Extend app for other use cases	Deliverables: None	Dates: None

Project: Application for JPEG privacy implementation with XACML	WP ref: (WP#) 2	
Major constituent: Testing and documentation	Sheet 5 of 5	
Short description: Testsing web app and proyect documentation	Planned start date:10-11-17 Planned end date: 25-01-18	
	Start event: 10-11-17 End event: 25-01-18	
Internal task T15: Testing Internal task T16: Documentation	Deliverables: None	Dates: None

1.4.2. Milestones

WP#	Task#	Short title	Milestone / deliverable	Date (week)
1	1,2,3,4	Search information	-	07-10-17
2	5,6,7,8	Design	-	15-10-17
3	9,10	Balana and create policies	Policies examples	10-11-17
4	11,12,13,14	Program main app	Application	18-12-17
5	15,16	Test and documentation	Final report	25-01-18

1.4.3. Gantt Diagram



Num	Task	Start	Final
1	Project scope	1-9-17	7-9-17
2	Search information about XACML	1-9-17	15-9-17
3	Search information about Balana	10-9-17	21-9-17
4	Investigate application JPEGMetadataEditor	14-9-17	26-9-17
5	Search information about MysQL and Image Storage	14-9-17	28-9-17
6	Search information about Java EE and Web App	14-9-17	30-9-17
7	Search information about Cryptography	18-9-17	2-10-17
8	Search information about Digital Signature	25-9-17	7-10-17
9	Use and adaptation JPEGMetadataEditor	25-9-17	8-10-17
10	Design new web application structure	8-10-17	15-10-17
11	Generation MySQL database	10-10-17	13-10-17
12	Definition storage for images	11-10-17	15-10-17
13	Create simple policies and request to check balana	20-10-17	3-11-17
14	Use balana to create an image authorization	3-11-17	10-11-17
15	First version of new application	1-11-17	18-11-17
16	Implement digital signature and encryption	18-11-17	25-11-17
17	Methodology to generate policies from requirements	25-11-17	30-11-17
18	Extend the application for other use cases	18-11-17	10-1-18
19	Testing	15-11-17	15-1-18
20	Documentation	3-12-17	15-1-18

Figure 1.4.3 : Gantt Diagram

1.5. Deviations and incidences

No major incidences have been found in the project, but some work packages have had to be modified to spend more time learning the XACML standard, which has been one of the bases of the project.

Finally the initial idea has been complemented by improvements and other points of view generated during the project.

2. State of the art

In this project, it uses technologies and implementations such as XACML standard [1] for the generation of privacy policies, Balana [2] as the engine that implements the architecture described in XACML and is able to analyze the entire process, it adds encryption for metadata security, it also includes a digital signature to ensure authenticity and finally complemented with WSO2 IS [3], software used as an editor to create policies.

2.1. XACML

XACML (eXtensible Access Control Markup Language) was ratified as an OASIS standard in 2003 and the latest version 3.0 was ratified in January 2013. XACML is a standard that implements a language for access control policies based on XML, was designed to become a universal standard for describing who has access to which resources. It also defines architecture for the interpretation of the policies that are generated. It also covers the request-response control protocol, which is based on how to create requests and how to manage the responses.

As the graph shows, the architecture that defines [4] the standard has the following structure:

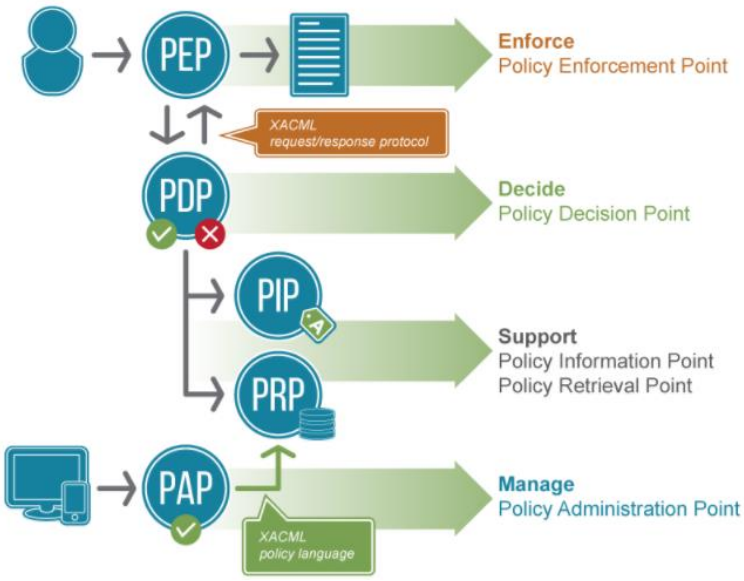


Figure 2.1 : XACML Architecture

PAP	Policy Administration Point - The system entity that creates or receive access policies
PDP	Policy Decision Point - Evaluate access requests against authorization policies before issuing access decisions
PEP	Policy Enforcement Point - Intercepts the user's request for access to a resource, demand a decision from the PDP to obtain the access decision
PIP	Policy Information Point - Entity that acts as a source of attribute values
PRP	Policy Retrieval Point - Stores XACML access authorization policies

2.2. Balana

Balana is an implementation of the architecture proposed by the XACML standard, therefore it defines tools to be able to work with the system described. The Balana project can be found in [2] where it consists of four modules:

1. Balana core – This is the actual implementation.
2. Balana samples – This contains the samples.
3. Balana Utils – This contains some utility methods in Balana.
4. Balana documentations – This contains docs.

2.3. Encryption and Decryption

The encryption of data and the use of encryption algorithms are fundamental for the security of an access control system, since they guarantee the invulnerability of communications between the devices that compose it.

Its use is essential to avoid attacks on the system, since they allow the information exchanged between the different elements to be completely undecipherable for non-users.

Advanced Encryption Standard (AES) [5] is one of the most widely used and secure encryption algorithms currently available. It started in 1997, when the NIST (National Institute of Standards and Technology) began looking for a successor to the standard DES encryption. The new AES encryption standard was officially announced in 2001.

The symmetric algorithm is based on several substitutions, permutations and linear transformations, each executed in blocks of data of 16 bytes. These operations are repeated several times, called "rounds". During each round, a unique circular key is calculated from the encryption key and incorporated into the calculations. The difference between AES-128, AES-192 and AES-256 is finally the length of the key: 128, 192 or 256 bits

2.4. XML Signature

The need to guarantee the integrity, confidentiality and authenticity of the data has become an essential requirement. To solve these problems, standards such as XML Signature [6] have been developed

XML Signature ensures the integrity of parts of transported XML documents.

It also provides authentication for data of any kind, whether it is in the XML that includes the signature or elsewhere. It can be applied to any digital content represented by XML. Primarily, XML Signature is to associate keys to the data.

XML Signature represents a system that through a digital signature allows offering authenticity of the data. The digital signature confirms the identity of the sender, the authenticity of the message and its integrity, without forgetting that the messages will not be disowned.

2.5. WSO2 Identity Server

WSO2 Identity Server is a product that allows us to manage the credentials and protocols of access to the resources and services of an entity through a single point of management. This solution allows us to manage all the internal authentication servers as if it were one only. WSO2-IS provides the most widely used access protocols in the market.

The product covers many tools for the management of privacy and security but in our case we are going to focus on the part related to XACML where it provides us with some policy editors and attributes management that we will use during the project.

3. Methodology / project development

The proposed solution for this project will be detailed, the objective is JPEG privacy implementation with XACML standard [7].

The project is divided into three phases in order to achieve the final objective, since apart from the privacy system that is the main purpose, we first need to design the privacy policies and then add them to the metadata.

- Creating Policies: Defines how privacy policies are created and designed.

- Updating Metadata: It is defined as adding the policies to the metadata of a JPEG image.

- Privacy System: The logic of the system that defines how a user requesting access to a JPEG image reaches its visualization through the integration of all components in an environment for user interaction.

3.1. Creating Policies

The first phase of this project is the creation of policies, so we are going to dedicate this part to the treatment and logic of this process.

One of the most important points of this project is the creation of privacy policies based on the XACML standard. XACML defines three top-level policy elements: <Rule>, <Policy> and <PolicySet>

Policy sets contains different policies. Policies are based on rules, each rule can have the effect of permit or deny.

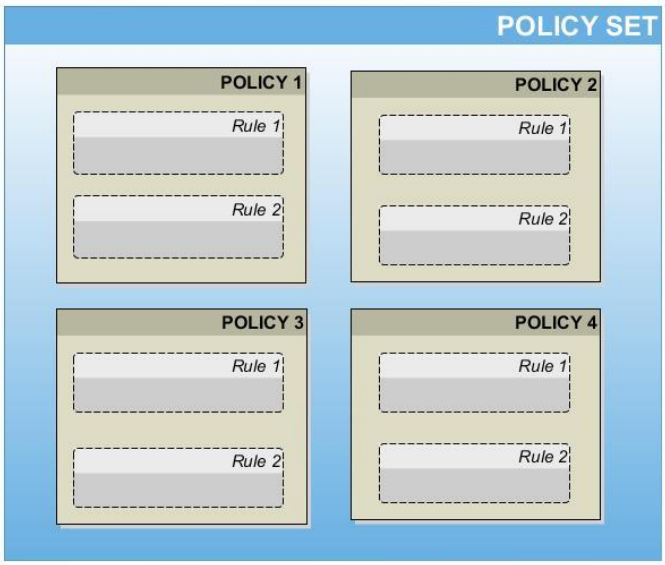


Figure 3.2 Policies Structure

An example in the figure above, the policy set includes four policies and each policy has two rules. XACML has a very high potential due to its easy scalability, it allows us to make very complex policies.

An important element is the combining algorithms that are used to solve conflicts between multiple policies and rules that are applied at the same time.

Combining algorithms must be used in:

- *PolicySet elements*
- *Policy elements*

The rule-combining algorithm defines a procedure for arriving at an authorization decision given the individual results of evaluation of a set of rules. Similarly, the policy-combining algorithm is used for a set of policies.

The most used Combining algorithms are listed below

- *Deny-overrides (Ordered and Unordered),*
- *Permit-overrides (Ordered and Unordered),*
- *First-applicable*
- *Only-one-applicable.*

Although there are other possibilities. (See XACML standard referenced for a full list of standard combining algorithms)

In the project, different policies were created without generating a set of policies, since it was not necessary for the final objective and we can work at the level of <Policy> as a

root element. So we are going to focus on the important element to make the decisions that are the rules.

A rule is the most elementary unit of policy and must be encapsulated in a policy. The main components of a rule are:

- **Description** – Documentation
- **Target** – Select applicable policies
- **Condition** – Boolean decision function
- **Effect** – Either “Permit” or “Deny”

Description; plain text with a brief description of the rule or policy that applies

Target; allows deciding if a rule applies to a request or not without evaluating the condition of the rule. In the case that it is NotApplicable, that rule or policy will have no effect for the response. If there are no other rules or policies that permit or deny, the response will be “NotApplicable”. It can be applied to different attributes. It is very important when creating Policysets and being able to filter which rules of all are evaluated according to the target.

Condition; this element sets the conditions that the request must satisfy to allow authorization. Attributes, functions and dataypes that are requirements of the designed policy are determined. It is possible to generate conditions also to deny access, so we have different ways of setting the rules.

Effect; The result of each rule is determined:

• If condition is true, return Effect value.

• If not, return Not Applicable.

• If error or missing data return Indeterminate.

3.1.1. XACML

In this chapter we are going to focus on the language with XACML code and to review how the project policies are created through code directly.

Once we have achieved a general knowledge of the XACML standard and the basic structure, we will see the creation of an XML policy using code to be used in our system.

In this case, the Eclipse editor has been used directly to create the policies. Eclipse is the software that we will also use to create the application to manage the privacy of the images.

The main structure of the policies designed is the following.

```
<Policy>
   <Description>
   </Description>
   <Target>
   </Target>
   <Rule>
      <Condition>
      </Condition>
   </Rule>
</Policy>
```

As we saw in the previous chapter, there is a <Policy> tag that encompasses the entire policy to be designed. The <Description> element will contain a brief explanation, and the <Target> that is used to define their scope, and finally the <Rule> with the element <Condition> inside, where we really determine what requirements the request has to satisfy to permit or deny access.

In order to complement these general tags and give functionality to our XACML structure code, we have syntax that we must use appropriately, there are many elements to use, but we will highlight those most used in our code and essential for designing policies.

Some of these elements as explained in the oasis XACML 3.0 standard.

"The `<Apply>` element denotes application of a function to its arguments."
"The `<AttributeValue>` contain a literal ***attribute*** value."
"The `<AttributeDesignator>` element retrieves a ***bag*** of values for a ***named attribute*** from the request ***context***."

Within these elements, the DataTypes, AttributesId, Categories and FunctionsID are detailed. It allows us to complete the functionality of the defined rules.

Example of policy with XML editor

Below is one of the policies we have generated for this project in XML code.The rule is applied in a business case.

"Only workers of the trading department during the month of November can access the image."

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy1_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides"
Version="1.0">
```

First, define the xmlns attribute that specifies the xml namespace for a document and a name for the Policy, in this case "Policy1_TFG". Also assign the type of the combinatorial algorithm for the rules of the policy, in the example is "permit-overrides" in the RuleCombiningAlgId attribute, that if any of the rules is permit, this will be the result of the policy, without taking into account the other rules.

```
<Description>All workers of trading department in November</Description>
```

Brief description about the use of this policy.

```
<Target>
  <AnyOf>
    <AllOf>
      <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        trading
        </AttributeValue>
        <AttributeDesignator AttributeId="department"
        Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
        DataType="http://www.w3.org/2001/XMLSchema#string"
        MustBePresent="true"/>
      </Match>
    </AllOf>
  </AnyOf>
</Target>
```

Next, the target of the policy is defined, it is required that the attribute department of the request be equal ("string-equal") to trading, in other case if the employee is from another department the policy will not be evaluated and it will return Not applicable for this request.

Also define the elements, MatchID, DataType, AttributeID, and Category with their respective URIS according to the requirement that must satisfy.

MustBepresent = "True" determines that it is an obligation to evaluate the target.

```
<Rule Effect="Permit" RuleId="PermitRule1">
   <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
               <AttributeDesignator AttributeId="department"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
            </Apply>
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
            trading
            </AttributeValue>
         </Apply>
```

```
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-greater-than">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
                  <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                  DataType="http://www.w3.org/2001/XMLSchema#date" MustBePresent="true"/>
               </Apply>
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">
               2017-11-01
               </AttributeValue>
            </Apply>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-less-than">
               <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
                  <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
                  Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
                  DataType="http://www.w3.org/2001/XMLSchema#date" MustBePresent="true"/>
               </Apply>
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">
               2017-11-30
               </AttributeValue>
            </Apply>
         </Apply>
      </Apply>
   </Condition>
</Rule>
</Policy>
```

Now, the code focuses on the body of a particular rule, in this case the rule that will allow us to access the image if we are in the month of November and the employee is from the trading department.

In this particular case we have two conditions to combine, using the conditional AND indicated by <Apply FunctionId = "urn:oasis:names:tc:xacml:1.0:function:and">. With this statement it is possible to combine two conditions in a rule.

Very similar to the target to establish that one of the conditions is the attributeID equal to department and trading as a value.

The other condition, in the month of November, but in this case dividing the condition in greater than the day 1-11-2017 and less than the day 30-11-2017. Applying the date-"greather-than" and "date-less-than" functions can be managed.

In this case, as a DataType, it is indicated as a date, with "DataType = http://www.w3.org/2001/XMLSchema#date".

Lastly, an additional rule is added in this policy,

```
<Rule Effect="Deny" RuleId="DenyRule"/>
```

A rule is defined without conditions that will always return the Boolean value as true, and "Deny" effect.

This rule is usually added for the case where the other rules are false, the output has a Deny effect and does not appear as NotApplicable

The "permit-overrides" algorithm will be imposed when a rule has a Boolean true and effect of rule permit, therefore it only has an effect in the case that the request does not satisfy any rule.

The definition of rules in XACML code can be complex for users without previous experience in this language, so a table has been proposed where the policy can be encapsulated in a visual and readable form in a simple way.

It can be seen that all the elements that are mentioned in the previous sections are indicated for design a policy, i.e: attributes, functions, datatypes, etc.

Category	Atributte	Type	FunctionID	Value	Condition

Policy defined with table:

POLICY 1 - permit-overrides					
RULE 1 - Permit					
Subject	Department	String	equal	trading	AND
Environment	Date	Date	greather-than	1/11/17	AND
Environment	Date	Date	less-than	30/11/17	END
RULE 2 - Deny					
No conditions	-	-	-	-	-
....					
-	-	-	-	-	-

Table 3.2.1 : Defined Policy

3.1.2. WSO2 Identity Server

In this chapter we focus on the usefulness of the WSO2 Identity Server platform, which through its editors facilitates the creation of policies.

The generation of rules directly in XACML language can be complex for users who do not have knowledge about XML language. The syntax can be confusing to create simple policies and rules, so it was decided to use a tool to define policies in a simple way.

After researching about XACML policy editors, we found a software created by WSO2 called WSO2 Identity Server that allows to create these policies and contain some other functions to help the management of privacy in an organization.

To be able to use this software, you can download it from its website [10] and then follow the steps [11] for installation.

```
C:\Users\Miguel\Desktop\wso2is-5.3.0\bin>wso2server.bat
JAVA_HOME environment variable is set to C:\Program Files\Java\jdk1.8.0_144
CARBON_HOME environment variable is set to C:\Users\Miguel\Desktop\wso2is-5.3.0
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=256m; support was removed in 8.0
```

Figure 3.2.2.A : Starting WSO2 server

We execute the script to configure a server in local host and its tools for our own use, we can access the system through the URL: https://localhost:9443/carbon/

This software has different editors to generate rules, we see the options after navigating on Home -> Entitlement -> PAP -> Policy Administration -> Add New Policy

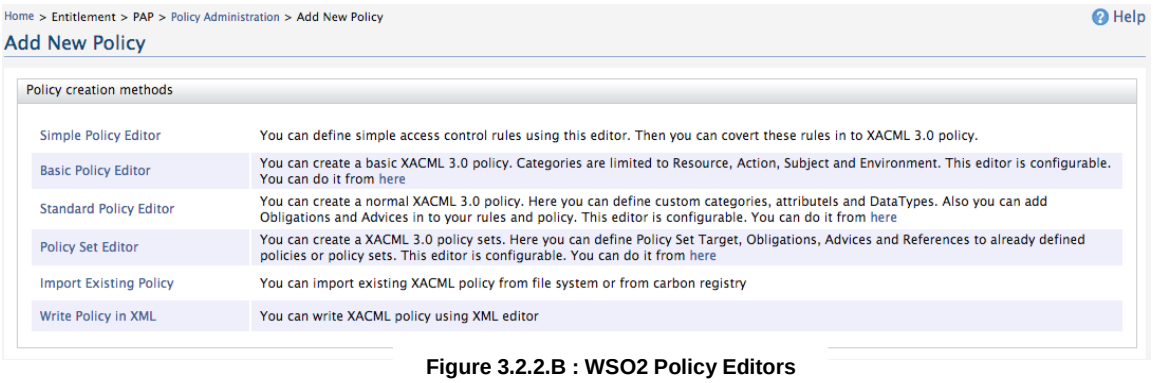


Figure 3.2.2.B : WSO2 Policy Editors

It has four editors that are valid for generating policies. In this project, the third option, the Standard Policy Editor, has been used.

The Standard Policy Editor is configurable and allows adding attributes, categories, datatypes, etc. It is flexible for our work if we want to have our own categories and attributes, and is also updated to the full version XACML 3.0.

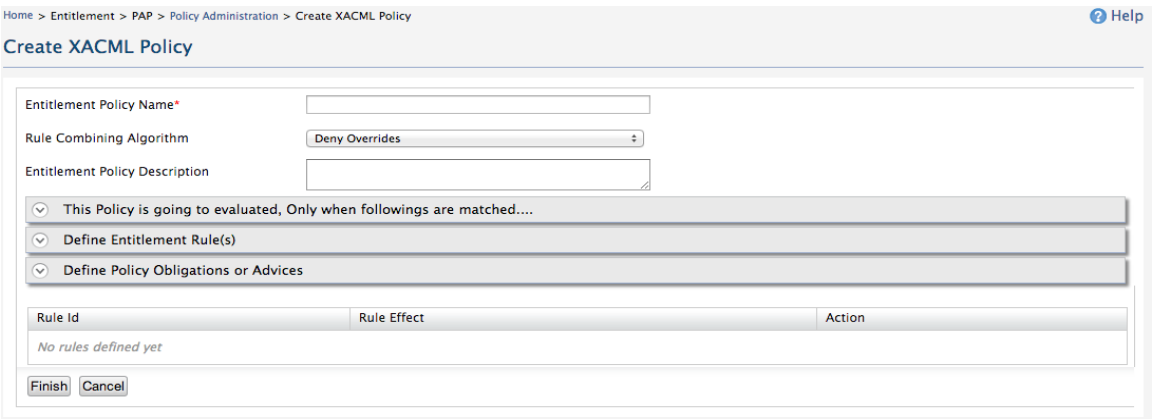


Figure 3.2.2.C : WSO2 Standard Policy Editor

In the image there is a first section to indicate the ID, the combining algorithm and the description of the new policy. After, three sections that are minimized, the first to put the

target, the second define the conditions and finally the possibility of adding obligations and advices.

We can see the example of the policy that we have made in XACML in the last chapter ,but in this case generated through this Standard Policy Editor.

<Policy> and <Description>

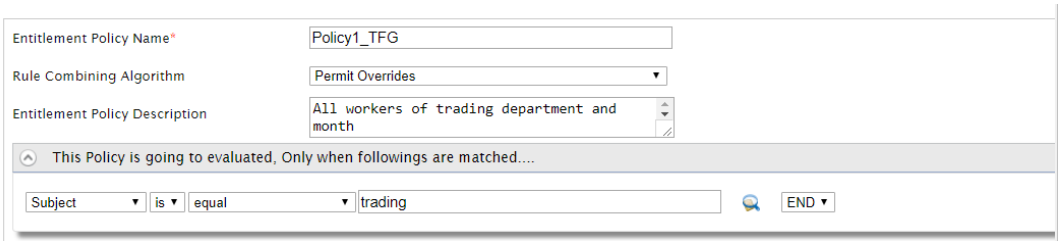


Figure 3.2.2.D : Description Policy Editor

<Target>

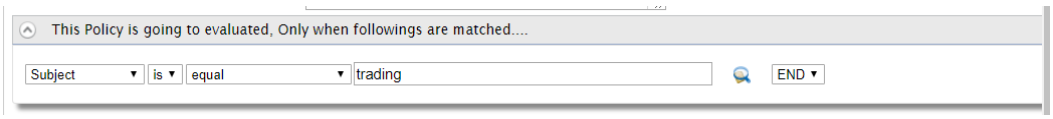


Figure 3.2.2 .E: Target Policy Editor

<Conditions>

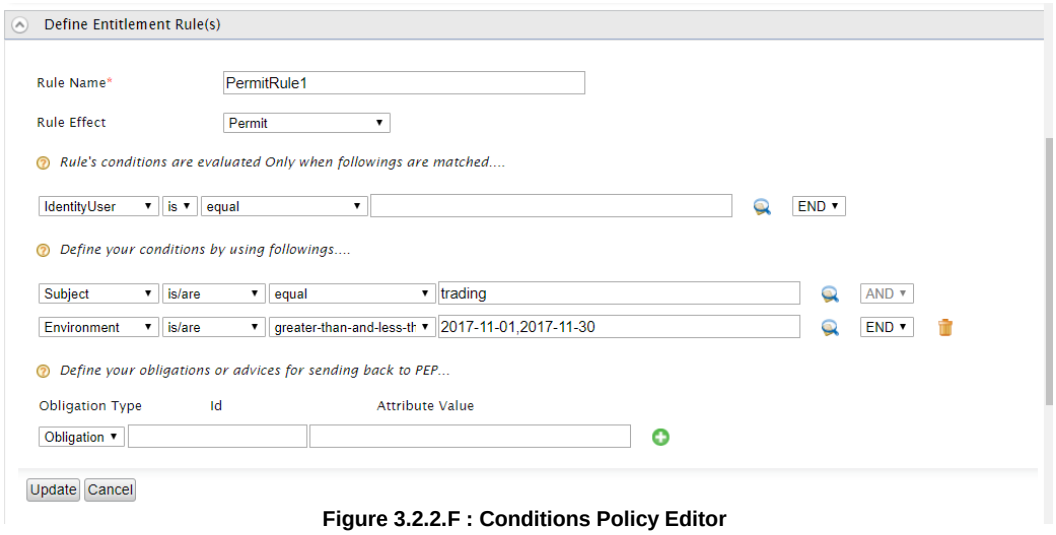


Figure 3.2.2.F : Conditions Policy Editor

In the lower part of the section we can navigate through all the rules of the policy to configure them:

Figure 3.2.2.G : Rules Policy Editor

We see that this software allows us to create policies easily and without having knowledge about the XACML language. Once created, we can obtain it directly expressed in XML in the "edit in xml" section.

Finally we will show how we can edit the policy editor to add options such as categories, attributes, datatypes, etc.

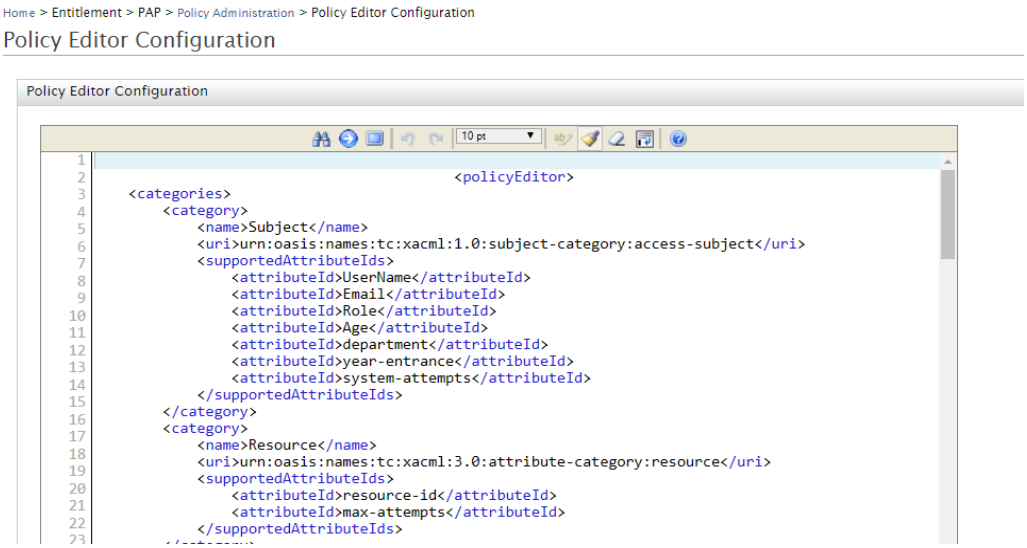


Figure 3.2.2.H : Configure Rules Policy Editor

For do this project, we have added to the category “Subject”, other attributes such as “department”, “year-entrance” or “system-attemps”, the same in Resource with “max-attemps”. It is shown in the previous figure.

To have these new attributes linked to the editor and generate correctly the URNs that we specify for generate a valid rules, we define them in the claims section of the software.

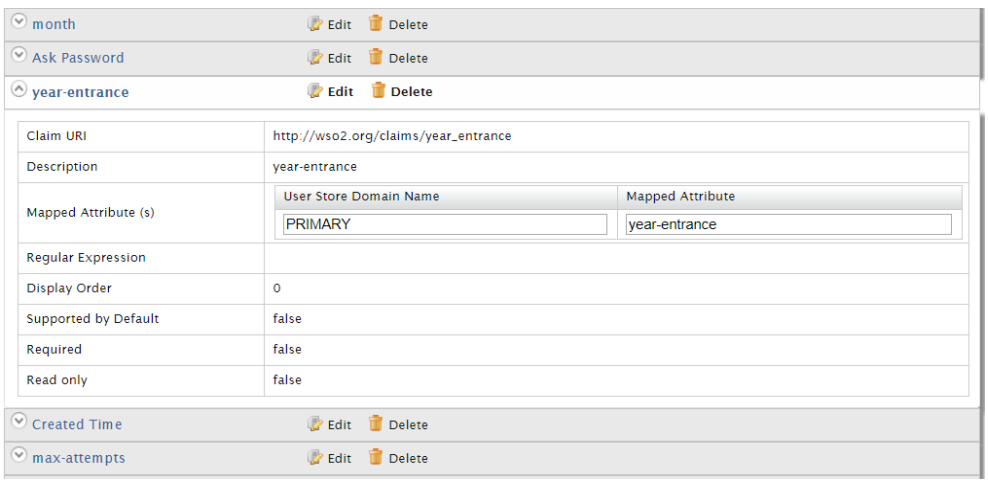


Figure 3.2.2.I : Add Attributes Policy Editor

3.2. Updating Metadata

In this chapter we start the second phase of the project where the objective is to add the created policies to the JPEG metadata. We will also include a digital signature in them.

Another of the main points of the project is where we will store the privacy policies of each image. One of the most compact and logical solutions is to add them to the metadata of the image [12]. The standardization of the metadata segment is currently being discussed to include a bookmark exclusively reserved for the management of privacy and security of the JPEG image.

3.2.1. JPSearch

JPEG Search (or JPSearch) [13] is an International Standard developed by the JPEG Committee (ISO/IEC JTC1 SC29/WG1). It specifies mechanisms to search for images, including metadata description.

The purpose of the standard is to provide common information in metadata in order to different systems be able to interoperate. It provides a flexible architecture for the search metadata and an extension is being developed to include the management of privacy and security in APP3 segment in metadata.

Our purpose is to use an existing field in the metadata of the JPSearch standard called Rights Description that allows us to include the privacy policies in the image metadata.

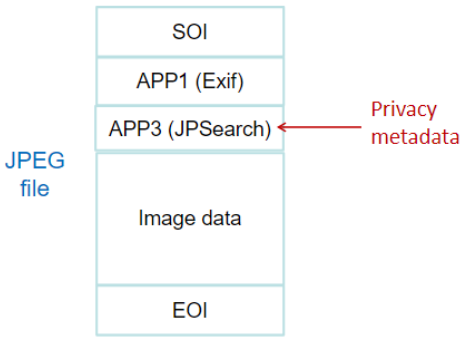


Figure 3.3.1 : JPSearch Segment

3.2.2. JPEGMetadataEditor

The JPEGMetadataEditor software is used to add the privacy policies in the JPSearch metadata. Initially developed [14] to modify metadata and later modified [15] for its adaptation to privacy metadata by means of the field Rights Descriptions.

The result provides a software with which it is possible to modify metadata and especially to take advantage of the Rights Description field to store a privacy policy with XACML code.

This program developed in java language had to be modified in this project to add the digital signature, since this feature was not included, in order to ensure the integrity and authentication of the metadata.

The following image shows the field where the XACML policy can be included with an example of privacy policy created for this project.

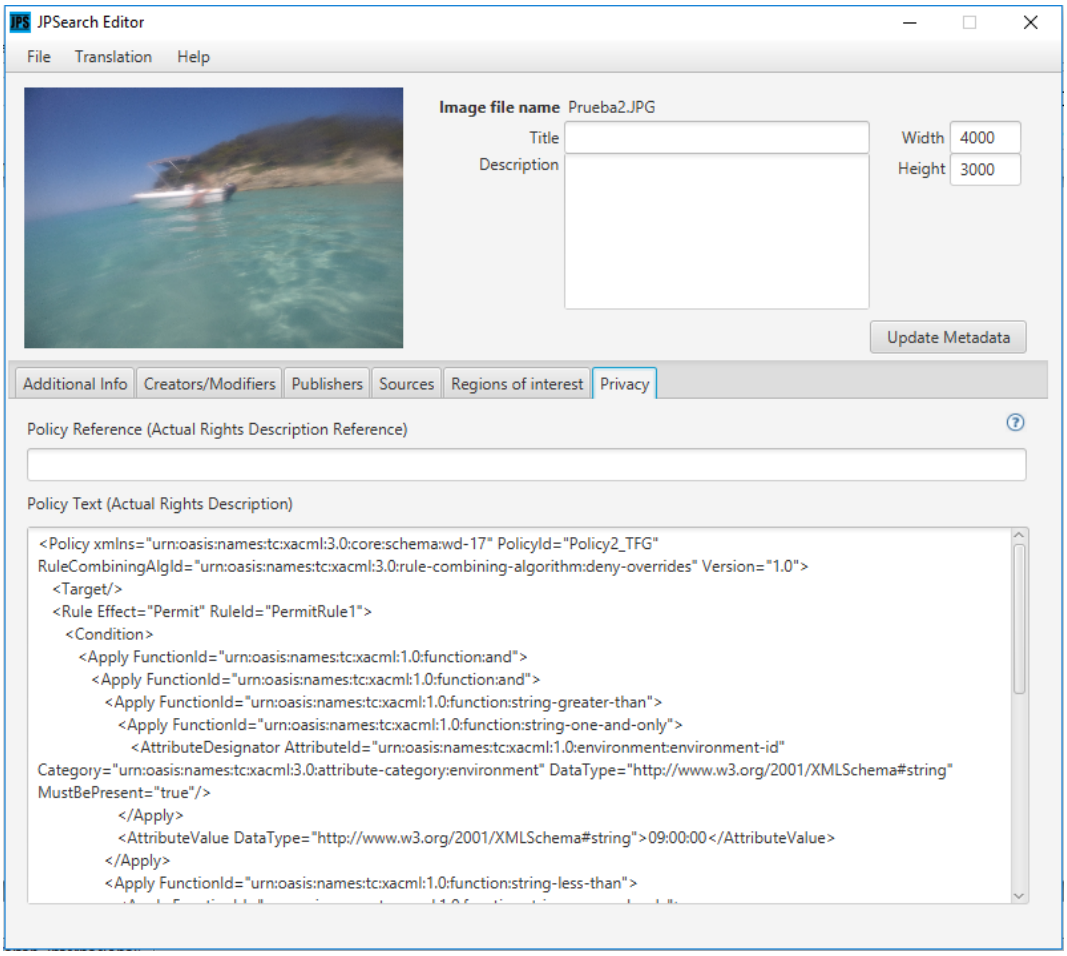


Figure 3.3.2: JPEGMetadataEditor

3.2.2.1. Insert policy

To enter a policy is done using the textbox provided by JPEGMetadaEditor in the privacy section, as shown in the previous figure.

Everything added in this field is collected in the Rights Description field of the metadata.

By attaching the XACML code of the policy in this space you can include the policy to the JPEG image.

This policy will be part of the metadata segment marker JPSeach called APP3, determined at the moment to contain the metadata privacy information.

3.2.2.2. Insert XML signature

Once the privacy policy has been introduced in this space, when updating the metadata with the "Update Metadata" button, an XML digital signature is added automatically in another field of the metadata.

The field in which we are going to include the signature is the labeling as "Keyword". It is defined in this project in this way, but it is currently being standardized which fields and which parts of the segment are going to really contain all this information about privacy in the future.

The digital signature XML is created in enveloped form. In this case, a signature is made using the DSA algorithm [16] and the hash function, SHA1, is added.

An example of a signature generated in the project is shown below.

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
        <Reference URI="">
            <Transforms>
                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>QHlmDFy3n2yowTKjR6PIACKr4ss=</DigestValue>
        </Reference>
    </SignedInfo>
    <SignatureValue>M9vmphqJn9WcwWXrVodS5ha2TFVKWEox6GdAnkr4xDwrEIGxicvOlA==
    </SignatureValue>
    <KeyInfo>
        <KeyValue>
            <DSAKeyValue>
                <P>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxeEu0ImbzRMqzVDZkVG9xD7nN1kuFw==
                </P>
                <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>
                <G>Z4RxsnqC9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==
                </G>
                <Y>Xj3kLTpFmzP8sdYOTTEt9+9NNPPgLaLsph+PxQ5i/BzeqpnHvRn8z0sc0h01lokr6lQefOhhKJiWTL6zspy3oQ==
                </Y>
            </DSAKeyValue>
        </KeyValue>
    </KeyInfo>
</Signature>
```

3.2.2.3. Encryption

At this point it is detailed how the encryption of the system is generated for greater security. The two fields of the metadata that we are going to encrypt are those that contain the privacy policy <RightsDescription> and the one that contains the digital signature <Keyword>.

Both fields are encrypted with symmetric encryption where the AES key is generated randomly coded with Base64 and the respective field is encrypted for each part, adding SHA 256 hash algorithm and finally encrypted with the AES standard.

The following image details how both fields are encrypted in the same way, we also have to remember as indicated in the previous chapter that the signature has its own asymetric encryption through DSA + SHA1. It is done internally in the field <SignatureValue>

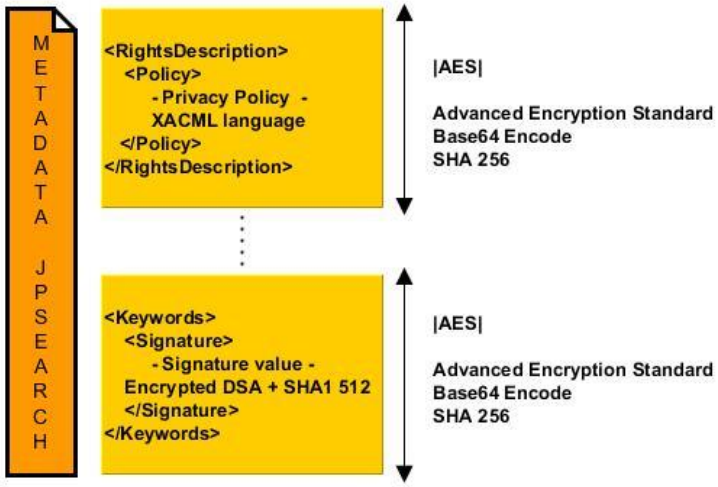
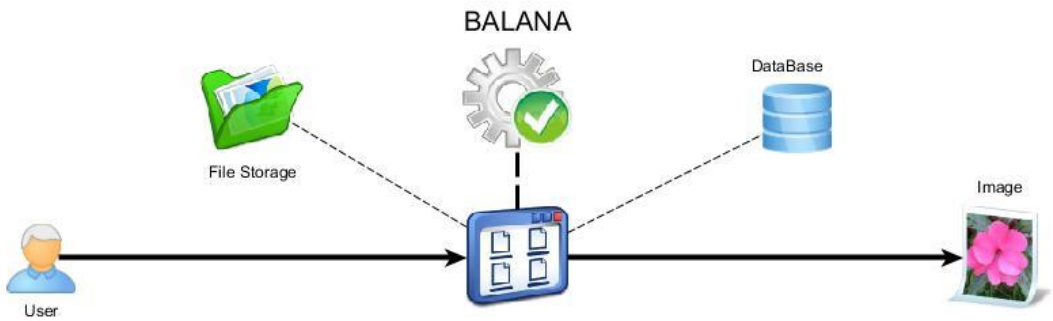


Figure 3.3.2.3: Encryption Schema

3.3. Privacy System

After the first two phases of the project, in this last phase, the application called Rights Validator will be designed, which will serve to close the project cycle and have a system capable to work with the designed policies and that we obtain through the metadata and implementing the Balana system for its validation.

To start developing this last part of the project we take into account an overview system as shown in the following figure.



3.3 : System Global Structure

The figure shows a horizontal central axis where the most basic structure of the system is defined; a user accesses the application and obtains an image.

For this process, the top part includes two main resources, storage for the images and databases. In addition, the core of the system is the Balana authorizer which will permit or deny access to the images requested by the user.

3.3.1. File Storage

A space is defined to store the images, specifically on the local disk. There are other solutions such as an external server or directly in the cloud to give the system more flexibility.

3.3.2. Databases MySQL

The necessary databases are also defined to store the information of both, the user who accesses the system and the information of the images. In this project we have worked directly with "MySQL Workbench" [8], a desktop application to manage MySQL [9] databases.

3.4. Core Structure Rights Validator App

The following schema shows the logic that has the core of the “Rights Validator” application developed in this project, starts with the selection and extraction of the metadata of the image to obtain the policy until the authorization through the Balana implementation to get the visualization of the desired image.

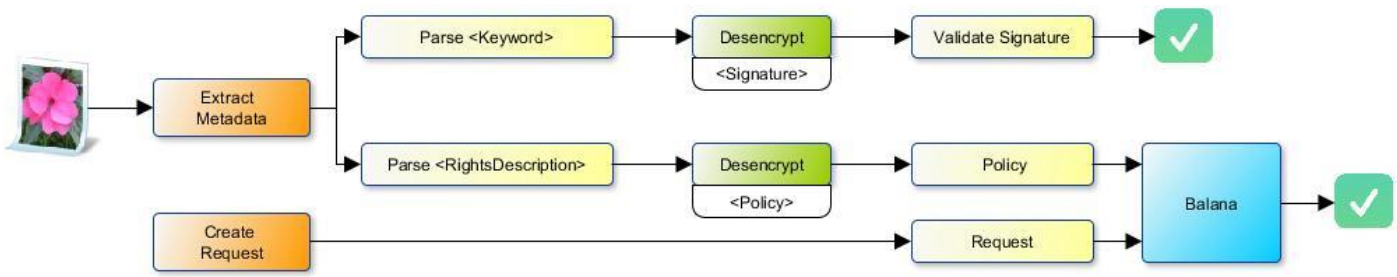


Figure 3.4: Core Structure Rights Validator

3.4.1. Login and Image Select

As an input to our system, a screen to perform the login through a username and password is displayed.

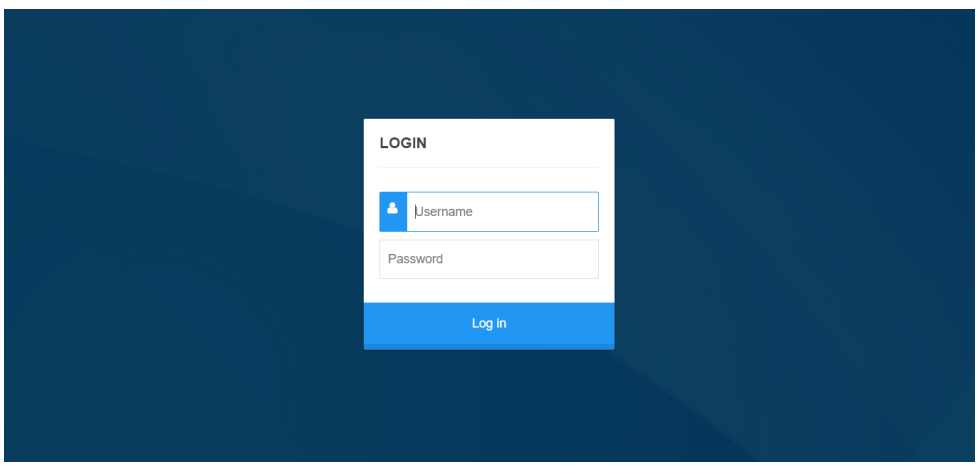


Figure 3.4.1.A: Login

First checking that the user trying to access the system is in the user database. If the access process is correct, the images contained in the database are shown to the user and so he can select the desired image to try to visualize it.

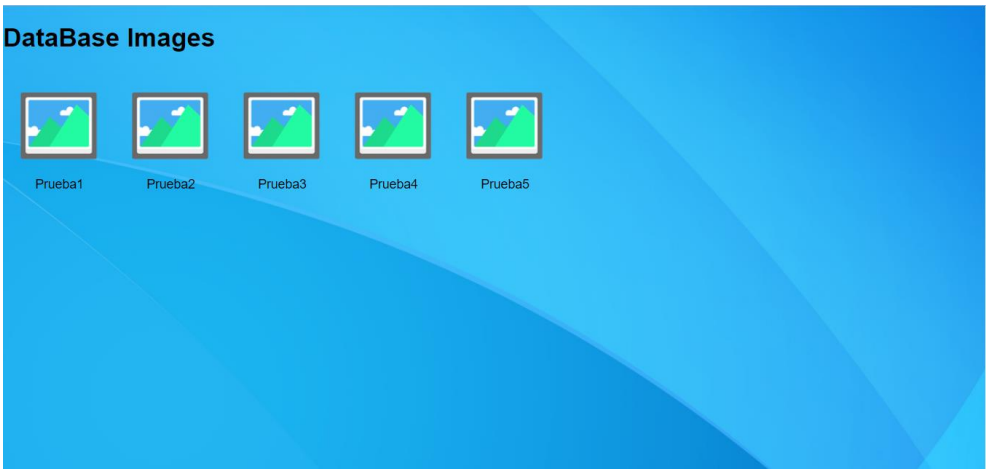


Figure 3.4.1.B: Image select

3.4.2. Extract Metadata

The user selects the desired image by clicking on the icon and the logic is executed to check if the user is valid to visualize the image.

The first step is the extraction of metadata from the image, which is provided by the JPSearch standard through the defined segment.

Once the bytes of the metadata are decoded to plain text, an XML format of all the metadata of the image is obtained, including the <Rights Description> and <Keyword> fields.

We see an example of extracted metadata from image in appendix A

3.4.3. Obtain Policy and Signature

Once we have extracted the metadata from the image, from the metadata we must obtain the required fields.

Previously commented that the <RightsDescription> fields that contain the privacy policy and <Keyword> that contains the digital signature are required, so by parsing the metadata in XML format, the two pieces of information are obtained in an encrypted form.

```
<RightsDescription>
    <RightsDescriptionInformation></RightsDescriptionInformation>
    <ActualRightsDescriptionReference></ActualRightsDescriptionReference>
    <ActualRightsDescription>xiqVOo95fjYThsyev+nH8uhmjhdW8X9iVYiAsjWGG97Wh+
    9ujhqlAokC2g/7XvQwHhvJGljucj54Wu4fj4WUjSi8NRJe8luT9xMiQQVyPTlalwmi95ADY
    hc6VANGi65YYeTEujq0oANGTBQ0MIbvCANflklZbGmLIYHevLJnH5Mc+u49+ZWU0/hPMGyc
                                                    ...
                                                    ...
                                                    ...
    bGmLIYHnH5Mc+evLJnH5Mc+u49+ZWU0/hPMGyc2duCggG6n6YDmjhdW8X9iVYiAsjWAflkl
    MIbvCANflklZMIbvCANflklZNR+nH5Mc+HjJU36ddIfE+VWf5toT4RmjSlRChVp/xILwqQ==
    </ActualRightsDescription>
</RightsDescription>
```

3.4.4. Decryption

The next step is the decryption of both the policy and the signature, using the inverse process to the one that performs the encryption in the JPEGMetadataEditor software.

Therefore, the privacy policy and the digital signature are available in XML format as originally created.

The application can now send to the validator the signature and the privacy policy to Balana for the validation and authorization process.

3.4.5. Validate XML Digital Signature

The digital signature is sent to the xml signature validator, where with the appropriate information contained in the fields <SignedInfo> and <KeyValue> it is possible to decipher the key for verification. In case the signature is valid, it will save a variable with a boolean to complement the final decision of the system. The XML digital signatures are important because add authentication, non-repudiation and data integrity, although the access permission is done through the privacy policy.

3.4.6. Generate Request

Another of the most important points of the system is the creation of the request that is compared with the privacy policy to permit or deny the visualization of the image selected.

The request is generated in a very similar way to the privacy policies with elements defined in the XACML standard. The main element is <Request>, within this element you can define the attributes that are required when defining a request according to the system and the designed policies.

For the generation of the request, this system is fed from the database, where three attribute classes are obtained.

- Attributes of the user (i.e :Name, Age, Department ...)

- Attributes of the image (i.e: Name, number of accesses ...)

- Environment attributes. (i.e :Date, time ...)

This can be related to some of the attributes that are specified in the XACML standard: Subject (User), Resource (Image), Environment (Environment), Action (view)

User attributes are saved when logging into the system. On the other hand, the attributes of the image are generated when selecting the desired image.

Finally, the attributes related to the environment are generated from the system itself. It can be summarized that the system has automatically made the request with the user's access information, the selected image information and system data information.

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
    <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
        <Attribute AttributeId="department" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeValue>
        </Attribute>
        <Attribute AttributeId="http://wso2.org/claims/role" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">senior</AttributeValue>
        </Attribute>
        <Attribute AttributeId="year-entrance" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2009</AttributeValue>
        </Attribute>
        <Attribute AttributeId="system-attempts" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">11</AttributeValue>
        </Attribute>
        <Attribute AttributeId="http://wso2.org/claims/age" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">28</AttributeValue>
        </Attribute>
    </Attributes>
```

```
    <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2</AttributeValue>
        </Attribute>
    </Attributes>
    <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">2018-01-08</AttributeValue>
        </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time" IncludeInResult="false">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">15:55:36</AttributeValue>
        </Attribute>
    </Attributes>
</Request>
```

3.4.7. Balana

Balana is an open source XACML implementation. This means that it is designed to fully support the standard, defining its data-flow model as specified.

The way that is used in this project is to indicate to Balana the directory where we have saved the policy extracted from the image and pass the request generated for the evaluation. In summary, the privacy policy extracted from the image and the request is delivered to Balana.

Balana establishes the implementation with the architecture defined by point 3.1 of the XACML standard:

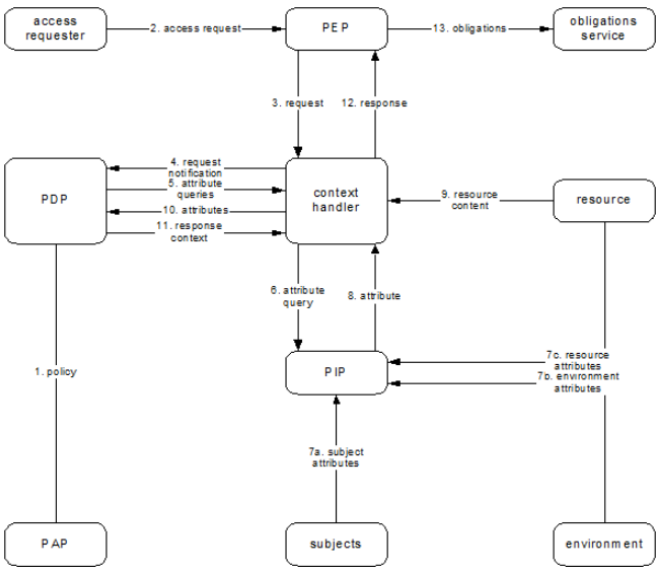


Figure 3.4.7: XACML standard architecture

Balana through its architecture based on the XACML standard, is able to verify that the request is valid or not for the privacy policy saved and will return a response with the final decision.

An example of response from Balana when the result is “Permit”:

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
    <Result>
        <Decision>Permit</Decision>
        <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok" />
        </Status>
    </Result>
</Response>
```

3.4.8. Display and Updates

In the final part of the application, a filtering is performed with the results of the digital digital signature and Balana's response about the privacy policy.

If the digital signature fails, an error appears with the text "Signature error" and the image is not displayed. On the part of Balana there is a decision in his response. Deny, Not Applicable or Indeterminate causes an error message where it shows the reason:

- Deny: the decision is in normal conditions, denying access because it does not comply with the privacy policy attributes.

- Not Applicable: The target of the policy does not match the request element, so the privacy policy does not apply to it.

- Indeterminate: Error in the syntax of the request or policy. It is possible a bad structure of elements or erroneous attribute.

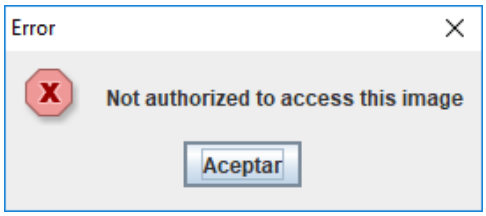


Figure 3.4.8.A: Deny display

Only in the case that the digital signature is valid and Balana's response is "Permit" the user will be shown a message indicating that have authorization to see the image.

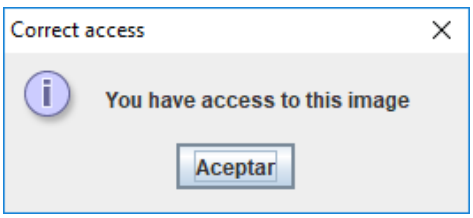


Figure 3.4.8.B: Permit display

Finally, some parameters of the database that are dynamic are updated as an example the times an image has been shown. So we can create policies that contain variable and updatable restrictions.

4. Results

The process of this project provides the "Rights Validator" application capable of acting as a privacy system for JPEG images through the policies defined in the XACML standard.

A system capable of validating and authorizing a request on an image of the database is implemented correctly, and allows viewing only if the conditions stipulated in the privacy policy contained in its metadata are correctly fulfilled.

For this purpose, another application defined in previous projects "JPEGMetadataEditor" is used to proceed with the integration of the privacy policy into the metadata. The digital signature has been adapted to this existing project since it did not include it.

In order to verify the satisfactory result of the application, two main points of the project have been analyzed: Design privacy policies and evaluate them in the authorizer.

4.1. Privacy policy design

It has been possible to design any type of privacy policy that has been needed through the XACML standard language, using a wide variety of elements provided by the standard. Versatility of this language has been proven by giving different policies with all kinds of attributes, datatypes, functions and decision algorithms. On the other hand, XACML native code is quite complex for a user that does not know the XACML language, another alternative has been presented that is to use an editor to create privacy policies. It has been used and demonstrated that can be created through open source software (WSO2 Identity Server) that allows us to create policies in a more friendly way.

For this reason, we believe that the expected results for the creation of policies have been fulfilled since we have not had any problems defining any type of requirement to formulate a policy. We have also proposed different ways to create policies.

In appendix B we find some of the main policies defined in the project.

4.2. Rights Validator App

The final result will determine if the application is able to correctly associate the available resources: images, databases, Balana implementation and the final decision for display or not the image.

To determine a result of the sequence that the application follows, it has been decided in each step that it takes to show the result it obtains in order to go through the entire architecture of the application and check the final decision according to our expectation.

Since the possible combinations for the verification are infinite, it has been decided to establish some concrete examples of inputs and to observe if the output is the expected one.

In all cases generated the expected response has been obtained, cases of "Permit" and "Deny" have been tested. You can check these tests performed in the next section.

In the appendix C you can check some examples of execution of the application.

4.3. Test 1

To perform a test in order to obtain valid and verified system results, a logic of access to the system and its respective requests to the images is defined.

In our environment created for the use case of a company and its employees there are 4 images defined with 4 different privacy policies. The first thing will be to know these policies and what users we have in the database.

The 4 images defined, with the purpose of their privacy policies are:

-Company1.jpg: All users of the trading department can access in the month of January 2018.

-Company2.jpg: Employees with year of entry to the company equal to or less than 2013 can access to the image between 9:00 a.m. and 5:00 p.m.

-Company3.jpg: It will be shown only to the first 3 users who access as trading department and senior role.

-Company4.jpg: Users with less than 26 years old or those with less than 2 accesses to the system.

On the other hand, the two tables that we have in the database for the company system are a reference for users and another for images.

idusers	user	pass	department	role	age	year_entrance	system_attempts	company
1	miguel	123	trading	senior	28	2009	0	xacml
2	jaime	123	finance	junior	36	2015	0	xacml
3	laura	123	trading	junior	26	2014	0	xacml
4	carlos	123	marketing	junior	25	2015	0	ext

4.3.1 Users company database

idimages	name	max_attempts
1	Company1	0
2	Company2	0
3	Company3	0
4	Company4	0

4,3.2 Images company database

With all this information we define a sequence of logins and accesses to images, we will note the result we expect in each of the iterations, finally we will complete the table by doing the sequence in our system and compare the expected result with the obtained one that should be the same.

The sequence to follow will be:

Login user miguel -> company1.jpg -> company2.jpg -> company3.jpg -> company4.jpg

Login user laura -> company4.jpg -> company1.jpg -> company3.jpg

Login user carlos -> company3.jpg -> company4.jpg -> company1.jpg

Login user miguel -> company3.jpg -> company3.jpg -> company3.jpg -> company4.jpg

Login user carlos -> company4.jpg

To assess the results we have defined a table with different fields to consider. The first is the type of access, if it is a login or an image request. Second the name of the resource or user who accesses. The next two show the expected and the obtained result. We also add the variables that will be updated in the system dynamically. We have the variable number of accesses to the system for the user and the maximum visualizations for an image, thus we create a more complex and sophisticated system. Finally the notes field, where the reason for the failed access is noted.

The table is as follows:

20/01/2017 at 20:17					
Type	**name**	**Result expected**	**Result obtained**	**Tables updates**	**Notes**
Login	miguel	-		miguel_sysatt = 1	
Request	Company1	Permit	Permit	company1_maxatt = 1	
Request	Company2	Deny	Deny		Time>17:00h
Request	Company3	Permit	Permit	company3_maxatt = 1	
Request	Company4	Permit	Permit	company4_maxatt = 1	
Login	laura	-		laura_sysatt = 1	
Request	Company4	Permit	Permit	company4_maxatt = 2	
Request	Company1	Permit	Permit	compant1_maxatt=2	
Request	Company3	Deny	Deny		Rol = junior
Login	carlos	-		carlos_sysatt = 1	
Request	Company3	Deny	Deny		Rol = junior
Request	Company4	Permit	Permit	company4_maxatt = 3	
Request	Company1	Deny	Deny		Departament = marketing
Login	miguel	-		miguel_sysatt = 2	
Request	Company3	Permit	Permit	company3_maxatt = 2	
Request	Company3	Permit	Permit	company3_maxatt = 3	
Request	Company3	Deny	Deny		maxatt>3
Request	Company4	Deny	Deny		system_att >1 and age >26
Login	carlos	-		carlos_sysatt = 2	
Request	Company4	Permit	Permit	company4_maxatt = 4	under 26 OK

4.3.3 Test summary table

After the simulation in our system gives us a result of 100% success as we expected. This test varies according to the time and day that the sequence is performed since we also have conditions such as date and time. In this case it was done on 01/20/2018 at 20:17

Tables with the variables updated at the end of the test:

idusers	user	pass	department	role	age	year_entrance	system_attempts	company
1	miguel	123	trading	senior	28	2009	2	xacml
2	jaime	123	finance	junior	36	2015	0	xacml
3	laura	123	trading	junior	26	2014	1	xacml
4	carlos	123	marketing	junior	25	2015	2	ext

4.3.4 Users updated company database

idimages	name	max_attempts
1	Company1	2
2	Company2	0
3	Company3	3
4	Company4	4

4,3.5 Images updated company database

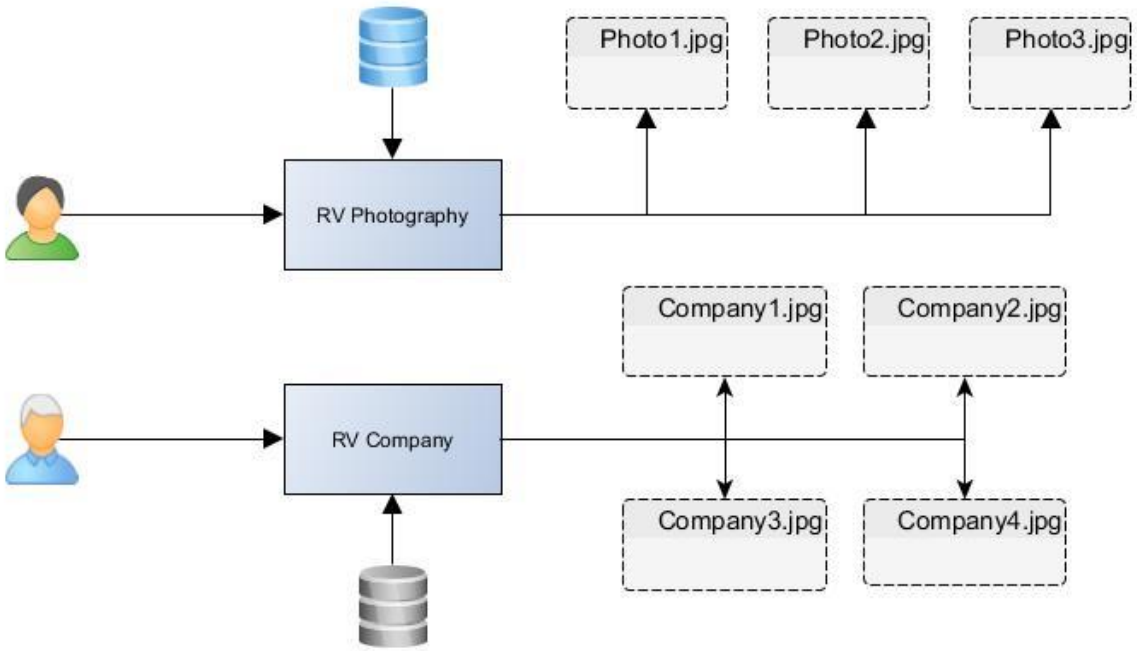
4.4. Another environment defined in the system

In the next section of the results, we want to show that the system designed for the JPEG image privacy management is universal and can be adapted to any type of environment that your service requires. Therefore, for any situation the general case is to have images and want to protect them through these privacy policies designed in XACML.

Then another case is established with different conditions and resources, since we are going to use other policies as well as other images and we will also obtain information from other databases to complete the requests to the system.

The previous environment was generated as a company with its employees and their own images that were uploaded to an internal intranet to share them.

In this case we are going to suppose that some photographers want to sell their images to users through the payment of a subscription and we want to control it with a system of privacy policies based on XACML.

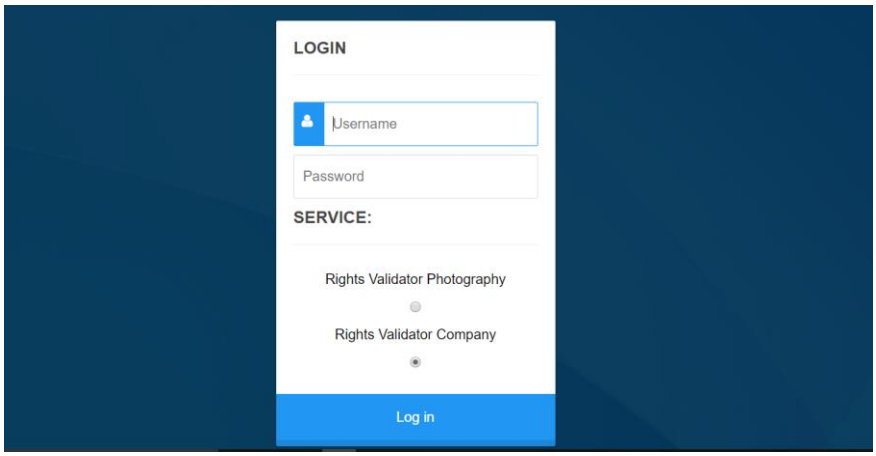


4.4.1 Schema of environments

In the graph we see how to access another generated system, with the same logic as the previous one, but changing the input users, the databases and the images hosted with different privacy policies.

Some parts have had to be duplicated to work independently and thus obtain greater abstraction from the rest of the system. The classes that create the request and access the data of the databases are different, but the main core of the system is the same and has not been modified.

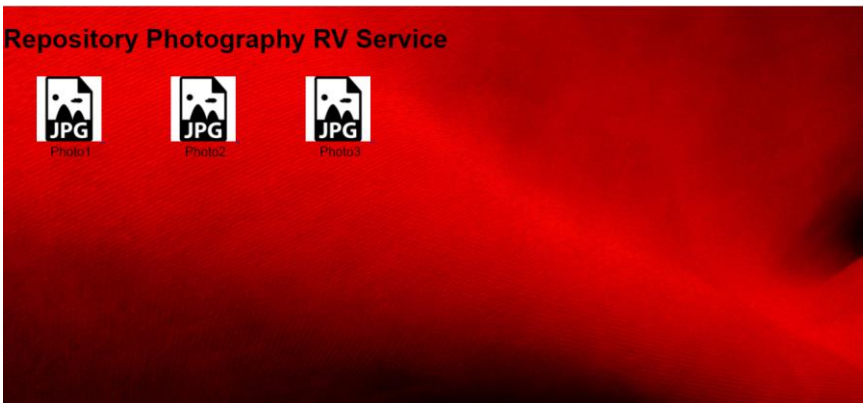
Now in the login you can choose the environment in which you want to work.



4.4.2 New login page

Selecting the "Rights Validator Photography" option will take us to the new environment created for your policy evaluation.

The images available in this environment are also displayed.



4.4.3 Images of new environment

As in the previous case, we will test the new environment in a sequence for the test.

4.5. Test 2

In this case we are going to simulate a sequence defined in the same way as in the first test carried out in the project but with the new users, images and information.

We define the three privacy policies designed in this environment:

-Photo1.jpg: Access for users from france or spain if they request access in the last 15 days of January

-Photo2.jpg: Users who have paid basic subscription can access if they are from the US and users who have paid the premium subscription from anywhere.

-Photo3.jpg: Any user who has paid their fee can access.

idusers	user	pass	paid	country	category
1	miguelimg	123	yes	spain	premium
2	jaimeimg	123	no	spain	free
3	lauraimg	123	yes	EEUU	basic
4	carlosimg	123	no	france	premium

4.5.1 Users Photography Database

idimages	name	creator	description
1	Photo1	Miguel	Photo1 Description
2	Photo2	Jaime	Photo2 Description
3	Photo3	Carlos	Photo3 Description

4.5.2 Images Photography Database

The following sequence has been generated to validate the results:

Login user miguelimg -> Photo1.jpg -> Photo2.jpg ->Photo3.jpg

Login user jaimeimg -> Photo1.jpg -> Photo2.jpg ->Photo3.jpg

Login user lauraimg -> Photo1.jpg -> Photo2.jpg ->Photo3.jpg

Login user carlosimg -> Photo1.jpg -> Photo2.jpg ->Photo3.jpg

In this case in the table results there is no field of updatable tables, because in this case we do not have variables that are updated by access or visualization, we certainly have variables that depend on a payment system to update, which would have to be done through another external service to confirm. In this case we have simulated it manually.

21/01/2017 at 00:27

Type	name	Result expected	Result obtained	Notes
Login	miguelimg	-		
Request	Photo1	Permit	Permit	
Request	Photo2	Permit	Permit	
Request	Photo3	Permit	Permit	
Login	jaimeimg	-		
Request	Photo1	Permit	Permit	
Request	Photo2	Deny	Deny	No paid free
Request	Photo3	Deny	Deny	No paid
Login	lauraimg	-		
Request	Photo1	Deny	Deny	EEUU no europe
Request	Photo2	Permit	Permit	
Request	Photo3	Permit	Permit	
Login	carlosimg	-		
Request	Photo1	Permit	Permit	
Request	Photo2	Deny	Deny	No paid premium
Request	Photo3	Deny	Deny	No paid

4.5.3 Test Summary Photography Table

It has achieved again 100% of expected results comparing with the obtained results, this test has been carried out in the following conditions: on 01/21/2018 at 00:27

As it has been highlighted in all the sections of the results, the overall and functional results of the system are satisfactory.

5. Budget

For this project, 542 hours have been worked. The software used is open source and free so no additional costs are added on this concept.

The salary of a junior engineer is in the current market around € 11 per hour, so this amount has been established in the table below.

Position	Amount	Hours	Price per hour	Total
Junior engineer	1	542	11 €	**5.962 €**

Table 5: Budget table

The personal computer is used so there are no hardware costs for estimating the budget

If you want to develop a global system with access from any terminal you would have to pay for a server and possibly some extra service such as a database or file storage in the cloud. The costs have been ignored since it has been worked as localhost.

6. Conclusions and future development

In the first part, the project started with the analysis of privacy policies from studying the XACML language, different policies and different forms of creation have been developed..

As a second part, the methodology for adding the policies and the digital signature to the metadata is generated from an existing application developed in previous projects. It has helped us to build the base of our "Rights Validator" application, since we needed JPEG images with privacy policies integrated in their metadata.

Finally, in the last part the application that defines the title of this project has been generated, an application for the privacy of JPEG images implemented from XACML, where we can validate the policies generated for different scenarios.

In conclusion, the main objective has been achieved, the application that allows us to manage the privacy of the images. It has also achieved the main goals that were originally proposed and others that were subsequently added, as a summary of these; a complete functional system, use XACML language, evaluate different incoming requests, integrate policies in the metadata, make practical examples of system use and include some security mechanisms such as encryption and digital signature.

For the future work, a more full system can be proposed that integrates the three parts treated, the policy creation, add these in the metadata and the validation system. The three modules in a single interface to be able to perform all the parts required by the user who accesses.

For this work you could establish an effective way to create a policy so that a user can easily incorporate it into their source image. Several tables/graphics are proposed during this project. These can be manipulated in a friendly way by a user who does not know the XACML language for the configuration of the policy in a visual form adding the fields

directly. Then it would have to convert to XACML code automatically from the table in order to integrate correctly in Balana.

Also take into account the source image so that the generated policy is automatically added to the metadata in the segment designed for this purpose of privacy and security. The signature should be added in the same way.

Table that collects attributes, functions, datatypes and everything necessary for the configuration of a policy in a friendly way.

POLICY 1 - permit-overrides					
RULE 1 - Permit					
Subject	Department	String	equal	trading	AND
Environment	Time	Date	greather-than	17:00	AND
Environment	Time	Time	less-than	21:00	END
RULE 2 - Permit					
Subject	Role	String	equal	senior	AND
Environment	Time	Time	less-than	21:00	END
RULE 3 - Deny					
-	-	-	-	-	-

Table 6.A: Policy Configuration Table A

Another type of distribution for the table that the user could modify easily.

POLICY 1			
RULE 1	**RULE 2**	**RULE 3**	**RULE 4**
Subject	***Subject***	***Subject***	***Environment***
Department	Role	Paid	Time
String	String	Boolean	Time
equal	equal	equal	greather-than
trading	senior	Yes	17:00
Age	***Environment***		***Resource***
String	Date		Resource-id
greather-than	Date		String
21	less-than		equal
Resource	02/05/2020		Photo
Resource-id			
String			
not equal			
Image			
Environment			
Date			
Date			
less-than			
01/01/2017	Rules definition		

Table 6.B: Policy Configuration Table B

Bibliography

[1] OASIS Standard, eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. Available : http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

[2] WSO2 Balana, License of Apache2, 30 November 2017 Available: https://svn.wso2.org/repos/wso2/trunk/commons/balana/.

[3] WSO2 Identity Server, Documentation, version 5.1.0, 2015-2017 Available : https://docs.wso2.com/display/IS510/About+Identity+Server

[4] Srijith Nair. "XACML Reference Architecture". 19 November 2013 Available: https://www.axiomatics.com/blog/xacml-reference-architecture/

[5] M.Pitchaiah, Philemon Daniel, Praveen, "Implementation of Advanced Encryption Standard Algorithm" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012

[6] XML Signature Syntax and Processing Version 1.1, W3C Recommendation 11 April 2013.

[7] Jaime Delgado, Silvia Llorente, "Improving privacy in JPEG images", in Proceedings of the IEEE International Conference on Multimedia & Expo Workshops (ICME), 2016. Avaiable : http://ieeexplore.ieee.org/document/7574676

[8] MySQL™ Workbench Reference Manual, Available : https://dev.mysql.com/doc/workbench/en/

[9] MySQL 5.1 Reference Manual, Available : http://www.mysql.com/5.1/reference

[10] WSO2 Identity Server, Software. Available : https://wso2.com/identity-and-access-management

[11] WSO2 Identity Server, Installation Prerequisites Available : https://docs.wso2.com/display/IS500/Installation+Prerequisites

[12] Benjamin Henne, Maximilian Koch and Matthew Smith, On the Awareness, Control and Privacy of Shared Photo Metadata, 2014.

[13] ISO/IEC, ISO/IEC 24800, Information technology – JPSearch, ISO/IEC. 2007 – 2012

[14] Demetriou, N., Delgado, J. (supervisor), Metadata Interoperability with JPSearch, http://www.slideshare.net/nikgt/metadata-interoperability-with-jpsearch, July 2013.

[15] Durán, A., Llorente, S. (supervisor), Privacidad en imágenes jpg mediante XACML (in Spanish), Final grade work, Barcelona School of Informatics (FIB), http://upcommons.upc.edu/handle/2117/82555, January 2016.

[16] Bojan R. Pajčin and Predrag N. Ivaniš, Analysis of Software Realized DSA Algorithm for Digital Signature, Electronics, Vol. 15, nº. 2, December 2011.

Appendix A

METADATA :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ImageDescription xmlns="JPSearch:schema:coremetadata">
    <Identifier>P5</Identifier>
    <Modifiers>
        <GivenName>Miguel </GivenName>
        <FamilyName>Castillo</FamilyName>
    </Modifiers>
    <Creators>
        <GivenName>Laura</GivenName>
        <FamilyName>Vilches</FamilyName>
    </Creators>
    <Publisher>
        <PersonName>
            <GivenName>Miguel </GivenName>
            <FamilyName>Castillo</FamilyName>
        </PersonName>
        <OrganizationInformation>
            <Name>TFG</Name>
            <Address>
                <Name>MCN</Name>
                <Description>MCN Company</Description>
            </Address>
        </OrganizationInformation>
    </Publisher>
    <CreationDate>2017-11-24T18:59:14.819+01:00</CreationDate>
    <ModifiedDate>2017-11-24T18:59:14.834+01:00</ModifiedDate>
    <Description>Beach</Description>
    <RightsDescription>
        <RightsDescriptionInformation>http://docs.oasis-
open.org/xacml/3.0/xacml-3.0-core-spec-os-
en.html</RightsDescriptionInformation>
        <Description>XACML3</Description>

<ActualRightsDescriptionReference></ActualRightsDescriptionReference>

<ActualRightsDescription>K8rUvKuf+f7p8LP9ckof5BGNGpbyIzybYHD9SEHXrz+ghgh
/XOtlY/4KOMMJKxCLDccaWbafbKfibMNW8Mfb2HHpkkQ72pGM38wIZKX8ixkU8bw+UCjlMbC
Ce0+d/QP2u+68B/EAZlAFWrWpEtQqY1nH7hvVZ352H/gbWrzr+FdKVAB5dfmgezSVe9Qy4iv
tt1WUrK0dBjdB6DeL/J5VZxjaBqTr1cLIQiTrn1LlNgVCs2kPSaILbizmT6zXY/WRCJCzLy6
YmIuK0AjQxC/rs8KMWUzs9t5oAldtXKpd23HlkeDi9dfhb+BJOd9k7Nsh3W7hShfQbErwWS1
pTAjCRuSYvYsnewbyw2gH483wrmo6YXNgXciu/g2eZRcEuwAuuriKDveltJdEDQ477SAX225
1Pk6D/2+4gorTbD0Huon5CxjV0eLC4ruuHMCy4g0jzNiNLSU1yTP63OSqI6pS/eEd5RCgy//
R8z7UFLGp5+57+RjgiKQDQrTGYz6QMVX2QXXLC/ZG1P7+Z67Ls3WmDLRxzwSaM/WpaWbLoP+
y7GWJWco2IqesFSJllcbyE9VcpppwKS1DGYki+rRCu6bR6PSpy2RSJDl20bpRwnxfTdZ2bjN
nwHONGX9MOXqw1B/oNGLcTayO7PzcP974s9t7qXt0gT1CRMr4tLQXs4BAWRAG/3QeWIXl19i
prUnGuo9HOpWOEPyXxcYqR9n3Ql2wwATl1JrS1/xPqAkEdHEn+gtPc5SsoTxyn0XoMz2isY4
O+Q+fbDsiSNhygSUKROJy6kmlpHNzzS80mWEKLC7sBBZsjpwoejLz2mfC5Kdu+dtejQz9qxb
fUC+xqsGszOpHtig8QP22orpAGHjDUmkI+eKTqTttKVnb9mP8Z5deactIrZNhfvLH/mEqYB8
lPxCtzj51kqhV3XLcga/wYdyM3cTK5JnEAp03jHEgJm/ngkdPa0jSu5GQ0THxIxQHVb6OrN0
/2rVo2liNLCvZEzBOQ/63BtduVDvFpsM89TZowQAxAYNmbPJcsZCe0F3trCQXSWO61bny/3N
gdEmo3QK3gGRmIcF/PCKEu+2WLOi1GrX8HZUzA7kZBMgxafEPMBUNAzc+hfsxEGHIJSDUAiM
DPx/I7FJHuaikxd4i8PlD5DXnHm24TMmT92OvweguDPioKDS6XzhsVafDHROSSGle5HfKJbN
zwXcO+w3Q0YFd6EnKu/bQl81EcBQRRsTYDxjLcQTcrj6Vj2x2BGvMArP3hZ0+P4GFt/0BoTL
ocjyBrgEyWYRCV2R0HEB75cnTiLsVs/Oc51G7XFg+smtESNO9Em6iS/v0d/WOWXYwsccZ2DL
x56BEekC1dERwUP4F7de2bjFjJkxFlaH0w1pqotdcuwtCaQJlOKz2NlJacmde5A</ActualR
ightsDescription>
    </RightsDescription>
```

```
    <Source>
        <SourceElementType>Camera</SourceElementType>
        <CreationMethod>Xiaomi Cam</CreationMethod>
        <CreationDescription>White 5"</CreationDescription>
    </Source>
    <Source>
        <SourceElementType>[Type]</SourceElementType>
        <CreationMethod>[Method]</CreationMethod>
        <CreationDescription>[Description]</CreationDescription>
    </Source>

<Keyword>O5dxywYWkrvyt09xbD5AvIlTWOMlbv0jlVs78Xehv9cYjXSrdCnsU4aHhmTq+Ni
JSOE+e0B1aepskq8f8pl5c0g0ch4ASuY6asSdyasAxf01R9Z+6cEsUD1EYl1sAIULMIdBewY
rupXQ/2bpa3dWoQ9VpBGo9eIJFAOFmq9P9x0x/ZKWUEilNL23jAxPtj+vXLpjk9pxZRoqlI/
0koBoxbGRTxvD5QKOUxsIJ7T539DxQFcNUb9Kc3w35FzbPctiIp7EpnJZXI3bu3VcdjWxAYg
PbrtSmjHDGGWawvqrUhNgpn0UF53TnFuILgRzzsRG/Ku8Q6cFdg+4ATAinpp2sRdn6+YaMB1
DcGIgZpjWh3e3/g8SYPq5/plcGb/fqpIj+0FVWYMsS6mLyroPAiUaLubuBYXXGMQkb0XIbhN
OvhFVQIFOEJERE0sTNDjvhsEBVGhKP+wsTlykEIaZrnVNQaNob1+nuYTH4rD36/8qAp9TSdm
9iQRFcThM1McImVxU3BfMClXZKZ6m5o9Lhr/bG+ekvXNA41CTaWlcCjT1RloAYEJVr5JA6Mj
4DjkTrQDgC5ClIvIS5S6zFwHySaXOIcEDc/hMaYJEtsEso0F/BoYyi6456z/net/fd6j5vsd
+B9ii8M2EzU2SFbYa8vPZHWF9KBUlteca5nyAeDywqiOTWAHXKdnvRCkybqFvMzXGwDaowrM
FqvL7vqSxRlZ746BkTZwunYJZXDXLQzgTz1CjKHUR03YGmANxg4XzgRpnqqVlqHvPEX8piOZ
XFp2v8vMUGw+dG25dX0//R81k4Q0spjBqZ73RSUJuwZiqvDR8ITESVqX6xP8iSjWGv+ukXuj
d4HYECXx/cIPmDUT0mjpqeC0OfbrP9XKdaVXzQqLILhGq8x0h9rRAqPmKrcd23OTZSSA3FmC
pXDeEO14FHdBEy9kEHViLtWy+SvHxke7inFYb2Y18CBrTt8C+kRAaKalgN2Eepo+X9zEd3+8
2oTq3XCcBYtzJv+sjRc1Pw0240xKBkRVFArw9pRE8UXeys/cA==</Keyword>
    <Title>Menorca</Title>
    <Rating>
        <LabelDefinition>Prueba</LabelDefinition>
        <LabelValue>P</LabelValue>
    </Rating>
    <OriginalImageIdentifier>
        <OriginationOfID></OriginationOfID>
        <Identifier>Prueba5</Identifier>
    </OriginalImageIdentifier>
    <GPSPositioning longitude="0.0" latitude="0.0" altitude="0.0"/>
    <RegionOfInterest>
        <RegionLocator>
            <Region dim="2">2200 713 3200 1463</Region>
        </RegionLocator>
        <Description>Its Miguel </Description>
        <Title>Person</Title>
        <ContentDescription/>
    </RegionOfInterest>
    <Width>4000</Width>
    <Height>3000</Height>
</ImageDescription>
```

Appendix B

Policy Image 1

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy1_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides" Version="1.0">
   <Description>All workers of trading department and
month</Description>
   <Target>
      <AnyOf>
         <AllOf>
            <Match
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeVal
ue>
               <AttributeDesignator AttributeId="department"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>
            </Match>
         </AllOf>
      </AnyOf>
   </Target>
   <Rule Effect="Deny" RuleId="DenyRule"/>
   <Rule Effect="Permit" RuleId="PermitRule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                  <AttributeDesignator AttributeId="department"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeVal
ue>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-greater-than">
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
                     <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#date" MustBePresent="true"/>
                  </Apply>
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2017-11-
01</AttributeValue>
               </Apply>
```

```
                <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-less-than">
                    <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
                        <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
DataType="http://www.w3.org/2001/XMLSchema#date" MustBePresent="true"/>
                    </Apply>
                    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#date">2017-11-
30</AttributeValue>
                </Apply>
            </Apply>
         </Apply>
      </Condition>
   </Rule>
</Policy>
```

```
</Policy>
```

Policy Image 2

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy2_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-overrides" Version="1.0">
   <Target/>
   <Rule Effect="Permit" RuleId="PermitRule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-greater-than">
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                     <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"

Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"

DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>
                  </Apply>
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">09:00:00</AttributeVa
lue>
               </Apply>
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-less-than">
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                     <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id"

Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment"
```

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"/>
                  </Apply>
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">17:00:00</AttributeVa
lue>
               </Apply>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                  <AttributeDesignator AttributeId="year-entrance"
                        Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"

DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="true"/>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2013</AttributeValue
>
            </Apply>
         </Apply>
      </Condition>
   </Rule>
   <Rule Effect="Deny" RuleId="DenyRule"/>

</Policy>
```

Policy Image 3

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy3_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides" Version="1.0">
   <Target></Target>
   <Rule Effect="Permit" RuleId="rule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-less-than">
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                     <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
                  </Apply>
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">3</AttributeValue>
               </Apply>
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                     <AttributeDesignator
AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
                  </Apply>
                  <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">senior</AttributeValu
e>
               </Apply>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                  <AttributeDesignator AttributeId="department"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeVal
ue>
            </Apply>
         </Apply>
      </Condition>
   </Rule>
   <Rule Effect="Deny" RuleId="DenyRule"></Rule>

</Policy>
```

Policy Image 4

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy4_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides" Version="1.0">
   <Target></Target>
   <Rule Effect="Permit" RuleId="rule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                  <AttributeDesignator
AttributeId="http://wso2.org/claims/age"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="true"></AttributeDesignator>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">26</AttributeValue>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
```

```
                <AttributeDesignator AttributeId="system-attempts"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="true"></AttributeDesignator>
              </Apply>
              <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
           </Apply>
        </Apply>
     </Condition>
  </Rule>
  <Rule Effect="Deny" RuleId="DenyRule"></Rule>

</Policy>
```

Appendix C

C.1 Example A

STEP 1 Metadata Extraction

METADATA :<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ImageDescription xmlns="JPSearch:schema:coremetadata">
<CreationDate>2017-11-19T21:31:20.827+01:00</CreationDate>
<ModifiedDate>2017-11-19T21:31:20.829+01:00</ModifiedDate>
<Description></Description>
<RightsDescription>
<RightsDescriptionInformation>http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html</RightsDescriptionInformation>
<Description>XACML3</Description>

<ActualRightsDescriptionReference></ActualRightsDescriptionReference>

<ActualRightsDescription>xiqVOo95fjYThs+ev+nH8uhmjhdW8X9iVYiAsjWGG97Wh+u
H4rupwVn7ihG60lXGCtlPQLKwRX6gYUDXF+S32sJ2Zyt2mCe5FZVxkJkmyxoOzQHu1pP6z3H
VVBWoQCX/LmFRJvurCQqFuCqkPqjpjRTPoGHYB73vsSPESyNZaMPV417yYR8D0RbwAqdRgpN
fkEAxmeFqJfhd90v5i1/9UpdoN6iz6E6pYtwOXh983hDNPXZo+90mA5hPBqEpUqmsZ9LyUO2
xMArURlHWzh9elUrc4Fqi+xhFtJRf9a3I27Uj9PBRWXfhID6d/VYNireTZhQrBvvX9bv9vKu
UbS429A/vT/nHCei7CwBRr/eLh1Ujp7ThoFG3gUNlloSWleJiYMtHHPBJoz9alpZsug/7LsZ
YlZyjYip6wVImWVxvIT1VymmnApLUMZiSL6tEK7ptLonv/+tjIPGWVKBgnmENbGVdXRi2ZYY
qO2MxPzjw8I3U30NRPXbjqD6edZeSuOyFtkLHk1biNczhr3sJ/YW6Mn8tYDthTcNTRuM69ig
zxGtx2j2mtZolq0aoSxAL/AjRI0cIpzNtGnn31pR5Vei1g/9G7bpbsRp67MxrBBIQMMqrgHc
gVV8pGts93smGoTyRaaEe7RO5gkAbFtAcSWA6TpqzRUgYx7ddQqD/bK8VLEO9OvXXSQEYKU+
7FfRHJZAOfbbnU+ToP/b7iCitNsPQe6ifkLGNXR4sLiu64cwLLiDSPM2I0tJTXJM/rc5Kojq
lT76+HVG0zQTmpEXNE3hsbeVXLwpBAsIKn9DV6EamE/jMxTrrmiN0+iuDsslWvyHzYFQrNpD
0miC24s5k+s12P11+XrXnAS2ikkKz5ojJdG37GE9Rv+aVyCjDUI3Cgoeysrc3xhUKH+Vt+Mf
YHkVdMkmsNrbynhyODnwXv+l46jBpX6Z7fd5kD7jkVQ0DP2R61gGPUhEpnixfn/jAtwT7vgF
ngOywJGiZeqjZ1LAySfyNd+Kl9h3KCl2WHidni6lwEyR6UBFyqINxFEvPuo1SlzgIGbN8cgS
c6x/TZgCM3VTr2b70+qnpDsRaWV3Vs72yuCWh76sxXJEMX4TzmWuP2yEEEtDQYDYEc3pgFgf
jg4nEmL3Yu5S4N5a404qttbAeKmgvv1xOPFLH5nTkZ0mHAb069ddJARgpT7sV9EclkA5eceb
bhMyZP3Y6/B6C4M+KtcKEYIewa+6e0m5UO9fCoT6xdnx1D+0ySn5P94z/BYJ26R4WGiAD1qR
FQP9EzWl4p+ehiMPSwleEl+crqDwGmo/o4FHZu6phX0XzN5q23awkbkmL2LJ3sG8sNoB+PN8
KzMU665ojdPorg7LJVr8h815x5tuEzJk/djr8HoLgz4pHiSFJ8qKogDjG9FUbCfxD9seMmiV
tqa4GLlYn9+EVAxTPoGHYB73vsSPESyNZaMNGyjHITwv6ORxRaDjWZMX7/aZ9xEMCpXeF2kC
aJ2G5zb069ddJARgpT7sV9EclkA59tudT5Og/9vuIKK02w9B7qJ+QsY1dHiwuK7rhzAsuINI
8zYjS0lNckz+tzkqiOqVPvr4dUbTNBOakRc0TeGxt5VcvCkECwgqf0NXoRqYT+MzFOuuaI3T
6K4OyyVa/IfNgVCs2kPSaILbizmT6zXY/XX5etecBLaKSQrPmiMl0bdhSXbMhXHF4XAk2f6j
+JQ8xscBCW9OWXd1WSsqbbqf4Qvh/tuxA08uNTE79v6vH+OhmjhdW8X9iVYiAsjWGG96k1cp
DDJMt7Fg0WCUIZjZQSkkCxWxFxs6qx0Wi9Yn0BIWhgUwnQn7gI+vzYcSe/Zm2Yy8I/745qBV
5KLk87Wpfn0d1SeXYxN78TZbKi1SlPHt9kfJj4phza6U4QYDN+dPYJ6TF1kwn5Yr/87HiA11
KdlOJDYY9KucN582LRW/XsssyNvYjpD2uPeBEA1Sreii+23VZSsrR0GN0HoN4v8nlVnGNoGp
OvVwshCJOufUuUz/rcG125UO8Wmwzz1NmjBADEBg2Zs8lyxkJ7QXe2sJBdJY7rVufL/c2B0S
ajdAreAZGYhwX88IoS77ZYs6LUas3zcMi19I1xWKH20uJ+9p9AHCldzjt9Zg09vHQS2+Es/H
8jsUke5qKTF3iLw+UPkNY1FU8KXx210CJgvgaH2NWxwWz4T4cyRhAGQuOTc9ki1e4ri1AHLu
XNNWjYpnxMc2dLosfbRPdbjFK6iqN8K0qEY0alvIjPJtgcP1IQdevP5hzXAUIEO2GPkzu4YK
75uiELo1IMye8tCAy/8ILqIuZkXH8xKICuRkF3tBV4SLlRyNHCKczbRp599aUeVXotYP/Ru2
6W7EaeuzMawQSEDDKq4B3IFVfKRrbPd7JhqE8kWmhHu0TuYJAGxbQHElgOk674KUvckqmPU/
7b0Y7d3oZCiMGJXMGKmxpN2Z3dFI5aYwp6P7gdL7lMmMT7rMJ3xqadojkzreGAWU3x21ul9K
b6uObj/XFBHaLhCj0jBLKp/qDZawJzbc4YuLsWhR4VG8upJpaRzc80vNJlhCiwu7AXkY7Zv0
eau7qg51gFZE6D2pf1pHquE4a6JSVEhfdoxTsEsnyxVWQdR3TpptxFZoJdukeFhogA9akRUD
/RM1peKfnoYjD0sJXhJfnK6g8BpopB/SCJG3aZNXHF3weKUphzL/f9xg8hiGbgfCqjOHOPkW

l7fTvo7Ij4/LaYNck410NKYleu96npnOwU2jDELClDvOvbN+3AHxVKvYxVxouCHT2tI0ruRk
NEx8SMUB1W+jl0Yrt6vXSKf80WkRI0l4fsdeg2MHgkaNu8bJUnLCY5kDc/hMaYJEtsEso0F/
BoYxFZgot0OC+Oxko2vHA/gKqbecZmjV2hDxoSZfV0UuSt4IrgdPQM2FtOFR1AT9mvqQO869
s37cAfFUq9jFXGi4IWrMcd9R30zLpWQdDj9c9Fl8k06/02YnaPg4qMj9VHdMSRGvLgJ8tT7l
h/KwZAxUvqzoA+MDJJhHsC4g/Ma6lRb63dF8buBnS395fYZN9VXFZnPakvyQOUSSJKng4jWl
ds4qHDPfmEpBIaf1zBZXPHPLvoZk8CTC3OPNarKiELvk=
    </RightsDescription>

<Keyword>O5dxywYWkrvyt09xbD5AvIlTWOMlbv0jlVs78Xehv9cYjXSrdCnsU4aHhmTq+Ni
JSOE+e0B1aepskq8f8pl5c0g0ch4ASuY6asSdyasAxf01R9Z+6cEsUD1EYl1sAIULMIdBewY
rupXQ/2bpa3dWoQ9VpBGo9eIJFAOFmq9P9x0x/ZKWUEilNL23jAxPtj+vXLpjk9pxZRoqlI/
0koBoxbGRTxvD5QKOUxsIJ7T539DxQFcNUb9Kc3w35FzbPctiIp7EpnJZXI3bu3VcdjWxAYg
PbrtSmjHDGGWawvqrUhNgpn0UF53TnFuILgRzzsRG/Ku8Q6cFdg+4ATAinpp2sRdn6+YaMB1
DcGIgZpjWh3e3/g8SYPq5/plcGb/fqpIj+0FVWYMsS6mLyroPAiUaLubuBYXXGMQkb0XIbhN
OvhFVQIFOEJERE0sTNDjvhsEBVGhKP+wsTlykEIaZrnVNQaNob1+nuYTH4rD36/8qAp9TSdm
9iQRFcThM1McImVxU3BfMClXZKZ6m5o9Lhr/bG+ekvXNA41CTaWlcCjT1RloAYEJVr5JA6M4
DjkTrQDgC5ClIvIS5S6zFwHySaXOIcEDc/hMaYJEtsEso0F/BoYyi6456z/net/4de0yoyNF
hMJdhp/nX2FyMc4zwPAB2sIjyT1CoGo1e/gJtQ8+iDThe5UWscm13H09wnOFWy3zPhgrRfKK
Z8ZugG/EfuSMnpCxXSl3L78bUjzijs6KCF3CH3GAytFTVjsWAaKu5dlfBiIJWclb5Pa934Wo
ce7zva5uYU5pWRlvitWwfv5o8UqCoxIhLN0W/9S2KRaQNowEMxVx++av1NpftGD+jrAy1kPR
CkybqFvMzXGwDaowrMFqvL7vqSxRlZ746BkTZwunYJZXDXLQzgTz1CjKHUR03YGmANxg4Xzg
RpnqqVlqHvPEX8piOZXFp2v8vMUGw+dG25dX0/1SQWRMzTTAx74jPJXoQPVbG1vUYRgPBiNc
C+iE4VJdlbjBbNBk0VzF9zX2d9sIuGMw9LQiV/yq5o/TzX6Dyx0EVx7QVgy/7jFCp3OFzouc
AJq5oZCiihvYMgAaQa0VMcVAMIsxvqh0SLLIO5bQn/T0vIzuAvbdP3baBfbBpgz6OX6FB8z1
IHqIO8BObgcnlgSYGK91M28LgwNXY7XbbxYpPkkw2V/R81k4Q0spjBqZ73RSUJuwZiqvDR8I
TWmIaRZ0SC/+kijq7Rz1r4YqPaIBuD0ZJxs0YNgnfCTJ5s1mUxzxZ1+nBYoAM0wT14W2cV5t
Xbfz2H6K6mjAoUfJoLGa6wUlm+48Gqyr5l16mL46KfAMHag/bHqRCDArqYb2Y18CBrTt8C+k
RAaKalgN2Eepo+X9zEd3+82oTq3XCcBYtzJv+sjRc1Pw0240xKBkRVFArw9pRE8UXeys/cA=
=</Keyword>

    <Title></Title>
    <Rating>
        <LabelDefinition></LabelDefinition>
        <LabelValue></LabelValue>
    </Rating>
    <OriginalImageIdentifier>
        <OriginationOfID></OriginationOfID>
        <Identifier></Identifier>
    </OriginalImageIdentifier>
    <GPSPositioning longitude="0.0" latitude="0.0" altitude="0.0"/>
    <Width>1920</Width>
    <Height>1080</Height>
</ImageDescription>

STEP 2 Encrypted <RightsDescription>:

Policy encrypted:

xiqVOo95fjYThs+ev+nH8uhmjhdW8X9iVYiAsjWGG97Wh+uH4rupwVn7ihG60lXGCtlPQLKw
RX6gYUDXF+S32sJ2Zyt2mCe5FZVxkJkmyxoOzQHu1pP6z3HVVBWoQCX/LmFRJvurCQqFuCqk
PqjpjRTPoGHYB73vsSPESyNZaMPV417yYR8D0RbwAqdRgpNfkEAxmeFqJfhd90v5i1/9Updo
N6iz6E6pYtwOXh983hDNPXZo+90mA5hPBqEpUqmsZ9LyUO2xMArURlHWzh9elUrc4Fqi+xhF
tJRf9a3I27Uj9PBRWXfhID6d/VYNireTZhQrBvvX9bv9vKuUbS429A/vT/nHCei7CwBRr/eL
h1Ujp7ThoFG3gUNlloSWleJiYMtHHPBJoz9alpZsug/7LsZYlZyjYip6wVImWVxvIT1Vymmn
ApLUMZiSL6tEK7ptLonv/+tjIPGWVKBgnmENbGVdXRi2ZYYqO2MxPzjw8I3U30NRPXbjqD6e
dZeSuOyFtkLHk1biNczhr3sJ/YW6Mn8tYDthTcNTRuM69igzxGtx2j2mtZolq0aoSxAL/AjR
I0cIpzNtGnn31pR5Vei1g/9G7bpbsRp67MxrBBIQMMqrgHcgVV8pGts93smGoTyRaaEe7RO5
gkAbFtAcSWA6TpqzRUgYx7ddQqD/bK8VLEO9OvXXSQEYKU+7FfRHJZAOfbbnU+ToP/b7iCit

NsPQe6ifkLGNXR4sLiu64cwLLiDSPM2I0tJTXJM/rc5KojqlT76+HVG0zQTmpEXNE3hsbeVX
LwpBAsIKn9DV6EamE/jMxTrrmiN0+iuDsslWvyHzYFQrNpD0miC24s5k+s12P11+XrXnAS2i
kkKz5ojJdG37GE9Rv+aVyCjDUI3Cgoeysrc3xhUKH+Vt+MfYHkVdMkmsNrbynhyODnwXv+l4
6jBpX6Z7fd5kD7jkVQ0DP2R61gGPUhEpnixfn/jAtwT7vgFngOywJGiZeqjZ1LAySfyNd+Kl
9h3KCl2WHidni6lwEyR6UBFyqINxFEvPuo1SlzgIGbN8cgSc6x/TZgCM3VTr2b70+qnpDsRa
WV3Vs72yuCWh76sxXJEMX4TzmWuP2yEEEtDQYDYEc3pgFgfjg4nEmL3Yu5S4N5a404qttbAe
Kmgvv1xOPFLH5nTkZ0mHAb069ddJARgpT7sV9EclkA5ecebbhMyZP3Y6/B6C4M+KtcKEYIew
a+6e0m5UO9fCoT6xdnx1D+0ySn5P94z/BYJ26R4WGiAD1qRFQP9EzWl4p+ehiMPSwleEl+cr
qDwGmo/o4FHZu6phX0XzN5q23awkbkmL2LJ3sG8sNoB+PN8KzMU665ojdPorg7LJVr8h815x
5tuEzJk/djr8HoLgz4pHiSFJ8qKogDjG9FUbCfxD9seMmiVtqa4GLlYn9+EVAxTPoGHYB73v
sSPESyNZaMNGyjHITwv6ORxRaDjWZMX7/aZ9xEMCpXeF2kCaJ2G5zb069ddJARgpT7sV9Ecl
kA59tudT5Og/9vuIKK02w9B7qJ+QsY1dHiwuK7rhzAsuINI8zYjS0lNckz+tzkqiOqVPvr4d
UbTNBOakRc0TeGxt5VcvCkECwgqf0NXoRqYT+MzFOuuaI3T6K4OyyVa/IfNgVCs2kPSaILbi
zmT6zXY/XX5etecBLaKSQrPmiMl0bdhSXbMhXHF4XAk2f6j+JQ8xscBCW9OWXd1WSsqbbqf4
Qvh/tuxA08uNTE79v6vH+OhmjhdW8X9iVYiAsjWGG96k1cpDDJMt7Fg0WCUIZjZQSkkCxWxF
xs6qx0Wi9Yn0BIWhgUwnQn7gI+vzYcSe/Zm2Yy8I/745qBV5KLk87Wpfn0d1SeXYxN78TZbK
i1SlPHt9kfJj4phza6U4QYDN+dPYJ6TF1kwn5Yr/87HiA11KdlOJDYY9KucN582LRW/Xsssy
NvYjpD2uPeBEA1Sreii+23VZSsrR0GN0HoN4v8nlVnGNoGpOvVwshCJOufUuUz/rcG125UO8
Wmwzz1NmjBADEBg2Zs8lyxkJ7QXe2sJBdJY7rVufL/c2B0SajdAreAZGYhwX88IoS77ZYs6L
Uas3zcMi19I1xWKH20uJ+9p9AHCldzjt9Zg09vHQS2+Es/H8jsUke5qKTF3iLw+UPkNY1FU8
KXx210CJgvgaH2NWxwWz4T4cyRhAGQuOTc9ki1e4ri1AHLuXNNWjYpnxMc2dLosfbRPdbjFK
6iqN8K0qEY0alvIjPJtgcP1IQdevP5hzXAUIEO2GPkzu4YK75uiELo1IMye8tCAy/8ILqIuZ
kXH8xKICuRkF3tBV4SLlRyNHCKczbRp599aUeVXotYP/Ru26W7EaeuzMawQSEDDKq4B3IFVf
KRrbPd7JhqE8kWmhHu0TuYJAGxbQHElgOk674KUvckqmPU/7b0Y7d3oZCiMGJXMGKmxpN2Z3
dFI5aYwp6P7gdL7lMmMT7rMJ3xqadojkzreGAWU3x21ul9Kb6uObj/XFBHaLhCj0jBLKp/qD
ZawJzbc4YuLsWhR4VG8upJpaRzc80vNJlhCiwu7AXkY7Zv0eau7qg51gFZE6D2pf1pHquE4a
6JSVEhfdoxTsEsnyxVWQdR3TpptxFZoJdukeFhogA9akRUD/RM1peKfnoYjD0sJXhJfnK6g8
BpopB/SCJG3aZNXHF3weKUphzL/f9xg8hiGbgfCqjOHOPkWl7fTvo7Ij4/LaYNck410NKYle
u96npnOwU2jDELClDvOvbN+3AHxVKvYxVxouCHT2tI0ruRkNEx8SMUB1W+jl0Yrt6vXSKf80
WkRI0l4fsdeg2MHgkaNu8bJUnLCY5kDc/hMaYJEtsEso0F/BoYxFZgot0OC+Oxko2vHA/gKq
becZmjV2hDxoSZfV0UuSt4IrgdPQM2FtOFR1AT9mvqQO869s37cAfFUq9jFXGi4IWrMcd9R3
0zLpWQdDj9c9Fl8k06/02YnaPg4qMj9VHdMSRGvLgJ8tT7lh/KwZAxUvqzoA+MDJJhHsC4g/
Ma6lRb63dF8buBnS395fYZN9VXFZnPakvyQOUSSJKng4jWlds4qHDPfmEpBIaf1zBZXPHPLv
oZk8CTC3OPNarKiELvk=

STEP 3 Decrypt <RightsDescription>:

Clean Policy:

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy3_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides" Version="1.0">
   <Target></Target>
   <Rule Effect="Permit" RuleId="rule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-less-than">
                  <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                     <AttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
                  </Apply>
```

```
                    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">3</AttributeValue>
                </Apply>
                <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                    <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                        <AttributeDesignator
AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
                    </Apply>
                    <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">senior</AttributeValu
e>
                </Apply>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                    <AttributeDesignator AttributeId="department"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
                </Apply>
                <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeVal
ue>
            </Apply>
        </Apply>
    </Condition>
  </Rule>
  <Rule Effect="Deny" RuleId="DenyRule"></Rule>
</Policy>
```

STEP 4 Encrypted <Keyword>:

Signature encrypted:

**O5dxywYWkrvyt09xbD5AvIlTWOMlbv0jlVs78Xehv9cYjXSrdCnsU4aHhmTq+NiJSOE+e0B1
aepskq8f8pl5c0g0ch4ASuY6asSdyasAxf01R9Z+6cEsUD1EYl1sAIULMIdBewYrupXQ/2bp
a3dWoQ9VpBGo9eIJFAOFmq9P9x0x/ZKWUEilNL23jAxPtj+vXLpjk9pxZRoqlI/0koBoxbGR
TxvD5QKOUxsIJ7T539DxQFcNUb9Kc3w35FzbPctiIp7EpnJZXI3bu3VcdjWxAYgPbrtSmjHD
GGWawvqrUhNgpn0UF53TnFuILgRzzsRG/Ku8Q6cFdg+4ATAinpp2sRdn6+YaMB1DcGIgZpjW
h3e3/g8SYPq5/plcGb/fqpIj+0FVWYMsS6mLyroPAiUaLubuBYXXGMQkb0XIbhNOvhFVQIFO
EJERE0sTNDjvhsEBVGhKP+wsTlykEIaZrnVNQaNob1+nuYTH4rD36/8qAp9TSdm9iQRFcThM
1McImVxU3BfMClXZKZ6m5o9Lhr/bG+ekvXNA41CTaWlcCjT1RloAYEJVr5JA6M4DjkTrQDgC
5ClIvIS5S6zFwHySaXOIcEDc/hMaYJEtsEso0F/BoYyi6456z/net/4de0yoyNFhMJdhp/nX
2FyMc4zwPAB2sIjyT1CoGo1e/gJtQ8+iDThe5UWscm13H09wnOFWy3zPhgrRfKKZ8ZugG/Ef
uSMnpCxXSl3L78bUjzijs6KCF3CH3GAytFTVjsWAaKu5dlfBiIJWclb5Pa934Woce7zva5uY
U5pWRlvitWwfv5o8UqCoxIhLN0W/9S2KRaQNowEMxVx++av1NpftGD+jrAy1kPRCkybqFvMz
XGwDaowrMFqvL7vqSxRlZ746BkTZwunYJZXDXLQzgTz1CjKHUR03YGmANxg4XzgRpnqqVlqH
vPEX8piOZXFp2v8vMUGw+dG25dX0/1SQWRMzTTAx74jPJXoQPVbG1vUYRgPBiNcC+iE4VJdl
bjBbNBk0VzF9zX2d9sIuGMw9LQiV/yq5o/TzX6Dyx0EVx7QVgy/7jFCp3OFzoucAJq5oZCii
hvYMgAaQa0VMcVAMIsxvqh0SLLIO5bQn/T0vIzuAvbdP3baBfbBpgz6OX6FB8z1IHqIO8BOb
gcnlgSYGK91M28LgwNXY7XbbxYpPkkw2V/R81k4Q0spjBqZ73RSUJuwZiqvDR8ITWmIaRZ0S

```
C/+kijq7Rz1r4YqPaIBuD0ZJxs0YNgnfCTJ5s1mUxzxZ1+nBYoAM0wT14W2cV5tXbfz2H6K6
mjAoUfJoLGa6wUlm+48Gqyr5l16mL46KfAMHag/bHqRCDArqYb2Y18CBrTt8C+kRAaKalgN2
Eepo+X9zEd3+82oTq3XCcBYtzJv+sjRc1Pw0240xKBkRVFArw9pRE8UXeys/cA==
```

STEP 5 Decrypt <Keyword>:

Clean Signature

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<body>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
                  <CanonicalizationMethod
                        Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315#WithComments" />
                  <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
                  <Reference URI="">
                        <Transforms>
                              <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                        </Transforms>
                        <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

      <DigestValue>QHlmDFy3n2yowTKjR6PIACKr4ss=</DigestValue>
                  </Reference>
            </SignedInfo>

      <SignatureValue>AHLtvJVlr3E81+HHqNXzxH7RIk9JSeEhOyLe6h2xz7KLgn+vsb
ya+A==</SignatureValue>
            <KeyInfo>
                  <KeyValue>
                        <DSAKeyValue>

      <P>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxeEu0Im
bzRMqzVDZkVG9xD7nN1kuFw==</P>
                              <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>

      <G>Z4RxsnqC9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5Bpsy4pNWM
OHCBiNU0NogpsQW5QvnlMpA==</G>

      <Y>lfOXRxcVjboo2avgjdpuU5KoBU9yNlc2NPgORKrS6EttPZKd10BLfkdFZELlYqp
SCqEFMc7WS9EeFLwnZQlKOA==</Y>
                        </DSAKeyValue>
                  </KeyValue>
            </KeyInfo>
      </Signature>
</body>
```

STEP 6 Validation Signature:

Signature passed core validation
2018-01-16
18:07:31

STEP 7 Generate Request:

Request:

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject">
<Attribute AttributeId="department" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">trading</AttributeVal
ue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/role"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">senior</AttributeValu
e>
</Attribute>
<Attribute AttributeId="year-entrance" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2009</AttributeValue>
</Attribute>
<Attribute AttributeId="system-attempts" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">16</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/age"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">28</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment">
<Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">2018-
01-16</AttributeValue>
</Attribute>
<Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">18:07:31</AttributeValu
e>
</Attribute>
</Attributes>
</Request>
```

STEP 8 Sending Policy to Balana:

STEP 9 Sending Request to Balana:

STEP 10 Balana Response:

Response:

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
      <Result>
      <Decision>Permit</Decision>
            <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
            </Status>
      </Result>
</Response>
```

STEP 11 Output Balana:

Final Decision: Permit

C.2 Example B

STEP 1 Metadata Extraction

METADATA :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ImageDescription xmlns="JPSearch:schema:coremetadata">
    <CreationDate>2017-11-20T00:12:51.148+01:00</CreationDate>
    <ModifiedDate>2017-11-20T00:12:51.149+01:00</ModifiedDate>
    <Description></Description>
    <RightsDescription>
        <RightsDescriptionInformation></RightsDescriptionInformation>

<ActualRightsDescriptionReference></ActualRightsDescriptionReference>

<ActualRightsDescription>xiqVOo95fjYThs+ev+nH8uhmjhdW8X9iVYiAsjWGG97Wh+u
H4rupwVn7ihG60lXGCtlPQLKwRX6gYUDXF+S32sJ2Zyt2mCe5FZVxkJkmyxpeKiMClHDOVz2
Kb21s1e4YLmFRJvurCQqFuCqkPqjpjRTPoGHYB73vsSPESyNZaMPV417yYR8D0RbwAqdRgpN
fkEAxmeFqJfhd90v5i1/9UpdoN6iz6E6pYtwOXh983hDNPXZo+90mA5hPBqEpUqmsZ9LyUO2
xMArURlHWzh9elUrc4Fqi+xhFtJRf9a3I27Uj9PBRWXfhID6d/VYNireTZhQrBvvX9bv9vKu
UbS429A/vT/nHCei7CwBRr/eLh1Ujp7ThoFG3gUNlloSWleJiYMtHHPBJoz9alpZsug/7LsZ
YlZyjYip6wVImWVxvIT1VymmnApLUMZiSL6tEK7ptpGp6tK2Iqy/bH7arKcYfmOZ18Kf9+ay
TWFcUvysYlSTOpnorWH6TKhWZPEjtgnYTsrc3xhUKH+Vt+MfYHkVdMr9nqeXi/U8ZZ8jVvCO
qPUNZCmJ5Emovo3enHxJPu02udPa0jSu5GQ0THxIxQHVb6MPHgbMvJuB7sHg5VmuBJTWMfC4
m7Ojv3YM7859aAgnbUK7h9sposDGWlGFc2f0pqglfv3eK+cf4+Fiz8RdglBPh85n1X3Zzlmi
wgEXpyYcfzMU665ojdPorg7LJVr8h86+PvtpmDkC7IA/sfNAM1+9iMVcytkYq8tX7GOzcJUp
H+P+Lr45/Rxe3b5LiVsA0klTyS7gHVwR73NyhpxiqsC51/5UPnUv5TDPflsIhD3fJFM+gYdg
Hve+xI8RLI1low5qkV5PzULgWmYMB40bxQ8J/0XIqOTEV+4fbGUjVYuRldDwcRXwavXtFkL4
GJMgQVHSWO61bny/3NgdEmo3QK3gGRmIcF/PCKEu+2WLOi1Grkf0WKxemLwZwusV3W+s0uIP
+L64gJZ+vgfH/OAPIE9IsFgQpKWHz3vjgTIW/WroBLrd8y5xBXN+GNOSVwGDysccFs+E+HMk
YQBkLjk3PZIvMxTrrmiN0+iuDsslWvyHzt2YxaqL3Q2DUjjvaY1bpgaY0pEGeOgZFVWT3fOP
91VuZLfEZX1xV2rNp1uVZbqaXmzL5Id5N7z4+Al9Uw8gqxlVT2YjhDI1IHube+V7QdX3fEhO
i0EKY95lxOxHIhIItKowQgOkJ4Tp5sPv1ZiUU6Di7MMDZc/wxX0SH/DBQlEDmLb4uJ2gMlpW
SBJAHROjW9HOpWOEPyXxcYqR9n3Ql216OAZgTCXQXWfke2Gfl/lqOTLWsccWMyj/WUDiioFh
ZUJcaqYsuXlLyYxAuRBgqh+Z18Kf9+ayTWFcUvysYlSTOpnorWH6TKhWZPEjtgnYTsrc3xhU
KH+Vt+MfYHkVdMr9nqeXi/U8ZZ8jVvCOqPUP7eFoxsPuaAxitX4D4EK/F5Ok5CtoMKaQvhVZ
```

EAbKvmhA7pAVvDp457/GGU7vhVpzoD3EgaKj2uzMDI44gCEL/cxNwKajP5trHQTpjnefnYaO
pl5Uo7GU/hInqu1UDmJr+YbHZ4J4vKgDRCN5VUVpXUK7h9sposDGWlGFc2f0pqoOKecmN2Gm
OUCW3SJy/KQFDR/8jinQnIP587Mx2gIPXzRhMrHd0i4CSd5PRbQfAXRdn6+YaMB1DcGIgZpj
Wh3cUHxM9DgtXNEvaintSQ6ILL5wTC3+iPbigP2rFGZRRBdQELJCd5YDkfIQNRIf8fn5VOgQ
PnjC+7KyBqf3r4da9dPa0jSu5GQ0THxIxQHVb6OrN0/2rVo2liNLCvZEzBOQ/63BtduVDvFp
sM89TZowQAxAYNmbPJcsZCe0F3trCQXSWO61bny/3NgdEmo3QK3gGRmIcF/PCKEu+2WLOi1G
r4w/zW2xE8zb9S7O/YIXFDPzg73xAoz2QVC4RF2VClMLKX4MPYC1a5VVtMp84jUbUNR+HjJU
36ddIfE+VWfzR3Q4poT4RmjSlRChVp/xUtwloS69lD1ar0qRa5b4kfHYxsqcWdDkX2NJ/t0k
bt5KY3lQwRPXj3s6SNlLjAz/gdLgUjK0GSbrcVBQiu2DnJmfbb8chJMtpnAEGLvgymqZp8rH
h3j0jlMoDkuGzGPgwMZo=
</RightsDescription>

<Keyword>O5dxywYWkrvyt09xbD5AvIlTWOMlbv0jlVs78Xehv9cYjXSrdCnsU4aHhmTq+Ni
JSOE+e0B1aepskq8f8pl5c0g0ch4ASuY6asSdyasAxf01R9Z+6cEsUD1EYl1sAIULMIdBewY
rupXQ/2bpa3dWoQ9VpBGo9eIJFAOFmq9P9x0x/ZKWUEilNL23jAxPtj+vXLpjk9pxZRoqlI/
0koBoxbGRTxvD5QKOUxsIJ7T539DxQFcNUb9Kc3w35FzbPctiIp7EpnJZXI3bu3VcdjWxAYg
PbrtSmjHDGGWawvqrUhNgpn0UF53TnFuILgRzzsRG/Ku8Q6cFdg+4ATAinpp2sRdn6+YaMB1
DcGIgZpjWh3e3/g8SYPq5/plcGb/fqpIj+0FVWYMsS6mLyroPAiUaLubuBYXXGMQkb0XIbhN
OvhFVQIFOEJERE0sTNDjvhsEBVGhKP+wsTlykEIaZrnVNQaNob1+nuYTH4rD36/8qAp9TSdm
9iQRFcThM1McImVxU3BfMClXZKZ6m5o9Lhr/bG+ekvXNA41CTaWlcCjT1RloAYEJVr5JA6M4
DjkTrQDgC5ClIvIS5S6zFwHySaXOIcEDc/hMaYJEtsEso0F/BoYyi6456z/net/4de0yoyNF
hMJdhp/nX2FyMc4zwPAB2sIjyT1CoGo1e/gJtQ8+iDThe5UWscm13H09wnOFWy3zPhgrRfKK
Z8ZugG/EfuSMnpCxXSl3L78bUjzijs6KCF3CH3GAytFTVjsWAaKu5dlfB8kY9a1hXA36p3Eo
8a3umjcFeseEpd22+PJ1TxwvN7cJ40SNFXHZ/oVrty6A7IUh/J/PGVfJnAZxs6L+X9Q1DnPR
CkybqFvMzXGwDaowrMFqvL7vqSxRlZ746BkTZwunYJZXDXLQzgTz1CjKHUR03YGmANxg4Xzg
RpnqqVlqHvPEX8piOZXFp2v8vMUGw+dG25dX0/1SQWRMzTTAx74jPJXoQPVbG1vUYRgPBiNc
C+iE4VJdlbjBbNBk0VzF9zX2d9sIuGMw9LQiV/yq5o/TzX6Dyx0EVx7QVgy/7jFCp3OFzouc
AJq5oZCiihvYMgAaQa0VMcVAMIsxvqh0SLLIO5bQn/T0vIzuAvbdP3baBfbBpgz6OX6FB8z1
IHqIO8BObgcnlgSYGK91M28LgwNXY7XbbxYpPkkw2V/R81k4Q0spjBqZ73RSUJuwZiqvDR8I
T7tiSWzGAozFOzTLt7iJm7523eEfxhfL6UI9y/LIMyORBQ7dF21DSCaqpgW8CN12SpPhUyTL
cpqdJxFd1Wdl2SJTZK0BjQdLQptcJIg+XDQFSsugPS/EzDDwNst79waYzYb2Y18CBrTt8C+k
RAaKalgN2Eepo+X9zEd3+82oTq3XCcBYtzJv+sjRc1Pw0240xKBkRVFArw9pRE8UXeys/cA=
=</Keyword>
<Title></Title>
<Rating>
<LabelDefinition></LabelDefinition>
<LabelValue></LabelValue>
</Rating>
<OriginalImageIdentifier>
<OriginationOfID></OriginationOfID>
<Identifier></Identifier>
</OriginalImageIdentifier>
<GPSPositioning longitude="0.0" latitude="0.0" altitude="0.0"/>
<Width>4608</Width>
<Height>3456</Height>
</ImageDescription>

STEP 2 Encrypted <RightsDescription>:

Policy encrypted:

xiqVOo95fjYThs+ev+nH8uhmjhdW8X9iVYiAsjWGG97Wh+uH4rupwVn7ihG60lXGCtlPQLKw
RX6gYUDXF+S32sJ2Zyt2mCe5FZVxkJkmyxpeKiMClHDOVz2Kb21s1e4YLmFRJvurCQqFuCqk
PqjpjRTPoGHYB73vsSPESyNZaMPV417yYR8D0RbwAqdRgpNfkEAxmeFqJfhd90v5i1/9Updo
N6iz6E6pYtwOXh983hDNPXZo+90mA5hPBqEpUqmsZ9LyUO2xMArURlHWzh9elUrc4Fqi+xhF
tJRf9a3I27Uj9PBRWXfhID6d/VYNireTZhQrBvvX9bv9vKuUbS429A/vT/nHCei7CwBRr/eL
h1Ujp7ThoFG3gUNlloSWleJiYMtHHPBJoz9alpZsug/7LsZYlZyjYip6wVImWVxvIT1Vymmn
ApLUMZiSL6tEK7ptpGp6tK2Iqy/bH7arKcYfmOZ18Kf9+ayTWFcUvysYlSTOpnorWH6TKhWZ
PEjtgnYTsrc3xhUKH+Vt+MfYHkVdMr9nqeXi/U8ZZ8jVvCOqPUNZCmJ5Emovo3enHxJPu02u

dPa0jSu5GQ0THxIxQHVb6MPHgbMvJuB7sHg5VmuBJTWMfC4m7Ojv3YM7859aAgnbUK7h9spo
sDGWlGFc2f0pqglfv3eK+cf4+Fiz8RdglBPh85n1X3ZzlmiwgEXpyYcfzMU665ojdPorg7LJ
Vr8h86+PvtpmDkC7IA/sfNAM1+9iMVcytkYq8tX7GOzcJUpH+P+Lr45/Rxe3b5LiVsA0klTy
S7gHVwR73NyhpxiqsC51/5UPnUv5TDPflsIhD3fJFM+gYdgHve+xI8RLI1low5qkV5PzULgW
mYMB40bxQ8J/0XIqOTEV+4fbGUjVYuRldDwcRXwavXtFkL4GJMgQVHSWO61bny/3NgdEmo3Q
K3gGRmIcF/PCKEu+2WLOi1Grkf0WKxemLwZwusV3W+s0uIP+L64gJZ+vgfH/OAPIE9IsFgQp
KWHz3vjgTIW/WroBLrd8y5xBXN+GNOSVwGDysccFs+E+HMkYQBkLjk3PZIvMxTrrmiN0+iuD
sslWvyHzt2YxaqL3Q2DUjjvaY1bpgaY0pEGeOgZFVWT3fOP91VuZLfEZX1xV2rNp1uVZbqaX
mzL5Id5N7z4+Al9Uw8gqxlVT2YjhDI1IHube+V7QdX3fEhOi0EKY95lxOxHIhIItKowQgOkJ
4Tp5sPv1ZiUU6Di7MMDZc/wxX0SH/DBQlEDmLb4uJ2gMlpWSBJAHROjW9HOpWOEPyXxcYqR9
n3Ql216OAZgTCXQXWfke2Gfl/lqOTLWsccWMyj/WUDiioFhZUJcaqYsuXlLyYxAuRBgqh+Z1
8Kf9+ayTWFcUvysYlSTOpnorWH6TKhWZPEjtgnYTsrc3xhUKH+Vt+MfYHkVdMr9nqeXi/U8Z
Z8jVvCOqPUP7eFoxsPuaAxitX4D4EK/F5Ok5CtoMKaQvhVZEAbKvmhA7pAVvDp457/GGU7vh
VpzoD3EgaKj2uzMDI44gCEL/cxNwKajP5trHQTpjnefnYaOpl5Uo7GU/hInqu1UDmJr+YbHZ
4J4vKgDRCN5VUVpXUK7h9sposDGWlGFc2f0pqoOKecmN2GmOUCW3SJy/KQFDR/8jinQnIP58
7Mx2gIPXzRhMrHd0i4CSd5PRbQfAXRdn6+YaMB1DcGIgZpjWh3cUHxM9DgtXNEvaintSQ6IL
L5wTC3+iPbigP2rFGZRRBdQELJCd5YDkfIQNRIf8fn5VOgQPnjC+7KyBqf3r4da9dPa0jSu5
GQ0THxIxQHVb6OrN0/2rVo2liNLCvZEzBOQ/63BtduVDvFpsM89TZowQAxAYNmbPJcsZCe0F
3trCQXSWO61bny/3NgdEmo3QK3gGRmIcF/PCKEu+2WLOi1Gr4w/zW2xE8zb9S7O/YIXFDPzg
73xAoz2QVC4RF2VClMLKX4MPYC1a5VVtMp84jUbUNR+HjJU36ddIfE+VWfzR3Q4poT4RmjSl
RChVp/xUtwloS69lD1ar0qRa5b4kfHYxsqcWdDkX2NJ/t0kbt5KY3lQwRPXj3s6SNlLjAz/g
dLgUjK0GSbrcVBQiu2DnJmfbb8chJMtpnAEGLvgymqZp8rHh3j0jlMoDkuGzGPgwMZo=

STEP 3 Decrypt <RightsDescription>:

Clean Policy:

```
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="Policy4_TFG"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:permit-overrides" Version="1.0">
   <Target></Target>
   <Rule Effect="Permit" RuleId="rule1">
      <Condition>
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                  <AttributeDesignator
AttributeId="http://wso2.org/claims/age"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="true"></AttributeDesignator>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">26</AttributeValue>
            </Apply>
            <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-less-than">
               <Apply
FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-one-and-only">
                  <AttributeDesignator AttributeId="system-attempts"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#integer"
MustBePresent="true"></AttributeDesignator>
               </Apply>
               <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
            </Apply>
```

```
        </Apply>
      </Condition>
   </Rule>
   <Rule Effect="Deny" RuleId="DenyRule"></Rule>
</Policy>
```

STEP 4 Encrypted <Keyword>:

Signature encrypted:

**O5dxywYWkrvyt09xbD5AvIlTWOMlbv0jlVs78Xehv9cYjXSrdCnsU4aHhmTq+NiJSOE+e0B1
aepskq8f8pl5c0g0ch4ASuY6asSdyasAxf01R9Z+6cEsUD1EYl1sAIULMIdBewYrupXQ/2bp
a3dWoQ9VpBGo9eIJFAOFmq9P9x0x/ZKWUEilNL23jAxPtj+vXLpjk9pxZRoqlI/0koBoxbGR
TxvD5QKOUxsIJ7T539DxQFcNUb9Kc3w35FzbPctiIp7EpnJZXI3bu3VcdjWxAYgPbrtSmjHD
GGWawvqrUhNgpn0UF53TnFuILgRzzsRG/Ku8Q6cFdg+4ATAinpp2sRdn6+YaMB1DcGIgZpjW
h3e3/g8SYPq5/plcGb/fqpIj+0FVWYMsS6mLyroPAiUaLubuBYXXGMQkb0XIbhNOvhFVQIFO
EJERE0sTNDjvhsEBVGhKP+wsTlykEIaZrnVNQaNob1+nuYTH4rD36/8qAp9TSdm9iQRFcThM
1McImVxU3BfMClXZKZ6m5o9Lhr/bG+ekvXNA41CTaWlcCjT1RloAYEJVr5JA6M4DjkTrQDgC
5ClIvIS5S6zFwHySaXOIcEDc/hMaYJEtsEso0F/BoYyi6456z/net/4de0yoyNFhMJdhp/nX
2FyMc4zwPAB2sIjyT1CoGo1e/gJtQ8+iDThe5UWscm13H09wnOFWy3zPhgrRfKKZ8ZugG/Ef
uSMnpCxXSl3L78bUjzijs6KCF3CH3GAytFTVjsWAaKu5dlfBi/z4b5s7p7ggFz6ee4fjbv6v
iq7Qi9IBiD+DYLwoAYrZlW4etJrlSSJnPO9exjUIRKl0koMI+hYXW6zYL4sBz/RCkybqFvMz
XGwDaowrMFqvL7vqSxRlZ746BkTZwunYJZXDXLQzgTz1CjKHUR03YGmANxg4XzgRpnqqVlqH
vPEX8piOZXFp2v8vMUGw+dG25dX0/1SQWRMzTTAx74jPJXoQPVbG1vUYRgPBiNcC+iE4VJdl
bjBbNBk0VzF9zX2d9sIuGMw9LQiV/yq5o/TzX6Dyx0EVx7QVgy/7jFCp3OFzoucAJq5oZCii
hvYMgAaQa0VMcVAMIsxvqh0SLLIO5bQn/T0vIzuAvbdP3baBfbBpgz6OX6FB8z1IHqIO8BOb
gcnlgSYGK91M28LgwNXY7XbbxYpPkkw2V/R81k4Q0spjBqZ73RSUJuwZiqvDR8IT1TSjpM51
NgQYK2MybqvQu3VIyz1N755KYE1mapM38Ftl3nnO/Dhj7jTW/LoIFw8dDyq2Vq3Ry915ViAc
y8yQ9plynkkYj++TqsP8pjB00rgMTH1vN9gtIaQecMTzqEOcYb2Y18CBrTt8C+kRAaKalgN2
Eepo+X9zEd3+82oTq3XCcBYtzJv+sjRc1Pw0240xKBkRVFArw9pRE8UXeys/cA==**

STEP 5 Decrypt <Keyword>:

Clean Signature

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<body>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
            <SignedInfo>
                  <CanonicalizationMethod
                        Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315#WithComments" />
                  <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1" />
                  <Reference URI="">
                        <Transforms>
                              <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                        </Transforms>
                        <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

      <DigestValue>QHlmDFy3n2yowTKjR6PIACKr4ss=</DigestValue>
                  </Reference>
            </SignedInfo>

      <SignatureValue>BotRKWC8dhK8ioO9JqX6XBVC+2c36mGb9V8kRHnfMnJ01nTMrd
vKhw==
            </SignatureValue>
            <KeyInfo>
```

```
                    <KeyValue>
                          <DSAKeyValue>

      <P>/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxeEu0Im
bzRMqzVDZkVG9xD7nN1kuFw==
                                </P>
                                <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>

      <G>Z4RxsnqC9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/XPaF5Bpsy4pNWM
OHCBiNU0NogpsQW5QvnlMpA==
                                </G>

      <Y>E+hUwNx98F1UxnJuwlibRhZXeX6YE9BNBks7KsBs/uoicqa7+0SKtYo8cauyMGs
+uRbk3Qz6ATyFz4ly1kn/eQ==
                                </Y>
                          </DSAKeyValue>
                    </KeyValue>
              </KeyInfo>
      </Signature>
</body>
STEP 6 Validation Signature:

Signature passed core validation
2018-01-16
18:23:31

STEP 7 Generate Request:

Request:<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
      CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject">
<Attribute AttributeId="department" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">finance</AttributeVal
ue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/role"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">senior</AttributeValu
e>
</Attribute>
<Attribute AttributeId="year-entrance" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">2001</AttributeValue>
</Attribute>
<Attribute AttributeId="system-attempts" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">2</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/age"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#integer">36</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:resource">
```

```
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id" IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">1</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment">
<Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#date">2018-
01-16</AttributeValue>
</Attribute>
<Attribute
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-time"
IncludeInResult="false">
<AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#time">18:23:31</AttributeValu
e>
</Attribute>
</Attributes>
</Request>
```

STEP 8 Sending Policy to Balana:

STEP 9 Sending Request to Balana:

STEP 10 Balana Response:

Response:

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
      <Result>
            <Decision>Deny</Decision>
            <Status>
            <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
            </Status>
      </Result>
</Response>
```

STEP 11 Output Balana:

Final Decision: Deny